NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

ORGANIZATIONAL STRUCTURE FOR INTER-AGENCY INFORMATION OPERATIONS

by

Richard K. Dougherty
and
Pablo F. Mir

March 2001

Thesis Advisor:	Carl R. Jones
Associate Advisor:	Thomas H. Gerblick

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2001	Master's Thesis

4. TITLE AND SUBTITLE :
Organizational Structure for Inter-Agency Information Operations

5. FUNDING NUMBERS

6. AUTHOR(S)
Dougherty, Richard K. and Mir, Pablo F.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

The purpose of this thesis is to stimulate a discussion toward developing an all-encompassing Inter-agency Information Operations organization. The authors define an environment and identify theories that point toward the necessity of integrating Information Operations (IO) throughout the U.S. Government (USG). The authors explore the feasibility of establishing and empowering an inter-agency organization that will monitor, evaluate and enforce all aspects of IO. Early forms of IO and their deployment are depicted in the historical backdrop of World War II. Concepts of renown futurists identify the importance of the Information Age and the essential process to maximize its' full potential. A correlation between the current national security strategy and the IO environment strongly suggests the need for innovation. An overview of the current IO environment and USG organizations reveals a technological move toward inter-agency IO. Both the art and science sides of IO are incorporated into a new organization. OrgCon 7.0 is used to analyze the proposed IO organizational structure, which provides specific recommendations and defines misfits that must be addressed. The authors conclude that further work is required in modeling the organization via alternate software and a more in depth look is required in the area of National Security IO. The authors provide the essential groundwork for further research.

14. SUBJECT TERMS
Information Operations, Inter-agency, Inter-departmental, Organization, OrgCon, National Security

15. NUMBER OF PAGES
242

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ORGANIZATIONAL STRUCTURE FOR INTER-AGENCY INFORMATION OPERATIONS

Richard K. Dougherty
Lieutenant, United States Navy
B.S., New York Maritime College, 1994

Pablo F. Mir
Lieutenant, United States Navy
B.S., United States Naval Academy, 1994

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2001

Authors: _____
Richard K. Dougherty

_____
Pablo F. Mir

Approved by: _____
Carl R. Jones, Thesis Advisor

_____
Thomas Gerblick, Associate Advisor

_____
Carl R. Jones, Chairman
Information Systems and Operations
Curriculum Committee

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis is to stimulate a discussion toward developing an all-encompassing Inter-agency Information Operations organization. The authors define an environment and identify theories that point toward the necessity of integrating Information Operations (IO) throughout the U.S. Government (USG). The authors explore the feasibility of establishing and empowering an inter-agency organization that will monitor, evaluate and enforce all aspects of IO.

Early forms of IO and its' deployment are depicted in the historical backdrop of World War II. Concepts of renown futurists identify the importance of the Information Age and the essential process to maximize its' full potential. A correlation between the current national security strategy and the IO environment strongly suggests the need for innovation.

An overview of the current IO environment and USG organizations reveal a technological move toward inter-agency IO. Both the art and science sides of IO are incorporated into a new organization. OrgCon 7.0 is used to analyze the proposed IO organizational structure, which provides specific recommendations and defines misfits that must be addressed. The authors conclude that further work is required in modeling the organization via alternate software and a more in depth look is required in the area of National Security IO. The authors provide the essential groundwork for further research.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The authors would like to acknowledge those individuals who provided their support throughout the process of this thesis. Special thanks to Dr. Carl Jones, COL Tom Gerblick, Dr. John Arquilla, and LT Ray Buettner for providing such solid wisdom and guidance while establishing a cornerstone of knowledge in the ever changing realm of Information Operations.

The authors would also like to extend thanks to fellow members of the inaugural Information Systems and Operations graduating class for their insights, professional experiences and solidarity.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS STATEMENT

In the wake of the Information Revolution, the numerous means of information exchange have exposed weaknesses that have been the source of much attention to include security, continuity, integrity and reliability. Although there are various methods and schools of thought to which information operations may be conducted, there must exist a cohesive policy and common structure from which those methods are employed. Policies, strategies and tactics all originate from an organization. Unfortunately, if an organization is stagnant, "old school" and unwavering in its' approaches to new problems, then it is fair to say that policies and therefore the methods in which we approach information operations will too be considered...obsolete.

B. MOTIVATION

In looking back through history, there exists three major shifts or "waves" in civilization to date. The First Wave dates back 10,000 years and is described as the "agrarian" age. It was during these first few thousands of years that civilization was dominated by nomadic wandering and hunting that evolved into farming and villages. The Second Wave began at the closing of the 18th century and is described as the "industrial revolution." The Second Wave brought the beginnings of steam, mass production, and modern machinery. The Third Wave involves the "information

revolution", which roughly began with the dawn of the space race in the 1950s. This period has experienced the birth of information technology plus social freedom and individuality. This brings us to where we stand today, in the middle of the information age. [Toffler, 1993] This is the model developed by Alvin and Heidi Toffler to depict where civilization has been, in hopes of predicting what the future may bring.

If the Information Age began nearly 50 years ago, why is it referred to as the "Information Revolution" today? Thomas Czerwinski expounds upon the Tofflers' theory, taking a deeper look into the in mechanics of the Third Wave. Czerwinski states that, "The Third Wave is not marked by a paradigm shift, but rather the lack of a paradigm." [Czerwinski, 1996] Czerwinski breaks down the composition of waves into three planes. The First Plane is inhabited by technology, artifacts and processes, which depict the economy, politics and social forms. The Second or "Intermediate" Plane describes the cultural aspects, such as art, literature, poetry, philosophy, and ideology. The Third Plane depicts the foundation, the fundamental ways of thinking. (See Table 1.)

Layer	1st Wave	2nd Wave	3rd Wave
Application	Agrarian	Industrial	Information
Interpretive	Premodernism	Modernism	Postmodernism
Foundational	Faith	Reason	Intuition

Table 1. Wave Composition [After: Czerwinski, 1996]

Historical studies support the concepts of Czerwinski and the Tofflers. First Wave wars were fought over land and natural resources. Second Wave wars while still fought over land, also targeted industrial centers and production plants. Warfare of the Third Wave still shows remnants of the First and Second Waves, but the focus is shifting toward the access and control of information. The United States, in its' brief history, depicts the transition through the waves. The economy of the United States, up until the late 18th century, was based upon land and natural resources. As the Second Wave approached, the economic wealth shifted toward industrial infrastructure. Today, in the thick of what is referred to as the "Information Revolution," the economy is once again shifting. The new wealth lies in knowledge, data and information along with the ability to store, transport and protect it.

It is the synchronization of the three planes (application, interpretive and foundational) that marks a complete shift from one wave to another. The First (application) Plane is represented by the advances in technology and processes. The economy has seen significant changes as the focus shift to information based companies. Politics have been challenged with issues such as the importance of privacy and the security of information. The Second (Intermediate or Interpretive) Plane has been altered in the appearance of information-based cultures. Art in the form of short films, music and literature are finding audiences on the Internet, where as they may have never been seen heard, or read before. The Internet has induced a flurry of new phrases and words that may one day be seen as shift in our language. The Age of Postmodernist thought may indeed be upon us.

> The primary goal of Postmodernists is to challenge convictions about the objectivity of knowledge, and the stability of language. They challenge the neutrality of science and the modern state and assert that their cognitive methods are biases by their agendas that are gendered, ideological and politicized....They also argue against the possibility of any certain knowledge. 'Truth' derives from the construct.... that human beings do not discover a truth in accordance with nature; they invent it, so the truth is always changing. [Appleby, Jacob & Hunt, 1995]

The Third (Foundational) Plane is still in progress and therefore, not entirely defined or understood. Czerwinski identifies the Age of Intuition as a concept based upon non-linear sciences.

> The hallmark of non-linear science is the startling idea that apparent chaos such as international relations, white water rapids, and battlefields, are unpredictable, but within bounds, self-organizing. [Czerwinski, 1996]

The Information Age has provided the opportunity to explore the idea of self-organization. This presents problems that must be solved. It is the synchronization of the three planes that will produce a genuine and complete shift into the Third Wave.

In 1996, the United States took another step toward the Third Wave. President Clinton signed The Clinger/Cohen Act, whose former title was the Information Technology Management Reform Act. This directs Federal agencies to establish a comprehensive approach toward managing the acquisition, use, and disposal of information technology. The act also ensures that Information Technology (IT) investments support strategic operational goals, and that delivery of services to the public are technologically up to date. The Clinger/Cohen Act established the position of Chief Information Officer (CIO) within each Executive Agency and tasked them with the responsibility of developing, maintaining, and facilitating the implementation of sound

and integrated IT enterprise architectures (EA). This act establishes the CIO council, made up of CIOs from all of the executive agencies. This council establishes the framework needed to completely integrate IO in the government. The focus is on the technology and science aspects of Information Operations. The CIO Council fails to integrate both the art and science sides of IO. This art side consists of soft perception techniques that range from public affairs to psychological operations. It is the fusion of art and science that is so essential in Information Operations.

C. THESIS GOALS

The overall goals of this thesis are to:

- Research and evaluate the current structures and policies of Information Operations (IO) at a Departmental/Agency level within the United States Government.
- Depict the current methods of how individual departments and agencies co-operate with each other in the realm of Information Operations.
- Identify inadequacies in the current Inter-Agency IO environment and propose legitimate corrective measures.
- Develop an organizational structure that will support solutions and remedies for the problems identified in the current environment.
- Analyze the proposed structure using Organization Consultant (OrgCon) 7.0 design software.
- Establish a solid foundation and provide recommendations from which future works may be endeavored.

D. THESIS ORGANIZATION & SUMMARY

This thesis is organized in to eight chapters. Each chapter is summarized as follows:

- Chapter I: Introduction. Identifies the purpose and motivation of the thesis. Establishes the thesis goals and objectives.

- Chapter II: Historical Reference: Depicts the importance of harnessing information operations via British and German intelligence agencies during World War II.

- Chapter III: Overview of Present Information Operations. Describes the current IO structures, down to the executive agency level and identifies deficiencies.

- Chapter IV: Relationship Between National Security, IO and Innovation. Examines current National Security policy and threats while focusing on the importance of Information Operations and innovation.

- Chapter V: Organizational Theory and Structure Methodology. Analyzes and describes key aspects and functional factors of organizational design.

- Chapter VI: Structure for the Inter-agency IO Council. Defines the proposed organizational structure, identifying major players, important relationships and general tasks.

- Chapter VII: Analysis of the Organization. Overview of Organizational Consultant (OrgCon 7.0) with the inputs, results and recommendations from the program.

- Chapter VIII: Future Considerations and Conclusion. Purposes thoughts and ideas of future considerations (possible future research) and closes the thesis via a conclusion.

THIS PAGE INTENTIONALLY LEFT BLANK

II. A HISTORICAL REFERENCE – WW II INFORMATION OPERATIONS

Information Operations (IO) was a key factor in the Allied victory in Europe. Although Information Operations was not the "official" term of the day, many operations that would be considered IO today, were conducted and conducted well. Communications were conducted via telegraph and radio. Radar, while used by both the Axis and the Allies, was still in its' infancy. Propaganda was widely used on both sides, both against the enemy and their own public. Deception, while not a new concept, had utilized the new technologies of the day. "All warfare is based on deception." [Sun Tzu, 1963, p.53] Communications, radar, propaganda, and deception all revolve around information. Between the Axis and the Allies, there was a battle for control of information and disinformation. These battles were fought between the intelligence agencies. The agency that could decode and manipulate the other's information while protecting their own would prevail. "It is often possible by adopting all kinds of measures of deception to drive the enemy in the plight of making erroneous judgments and taking erroneous actions, thus depriving him of his superiority and initiative." [Sun Tzu, 1963, p. 53]

A. BRITISH INTELLIGENCE

In the early parts of World War II, Winston Churchill recognized the importance of a solid intelligence network and the role that it would play in the defeat of the Axis countries. It is with this knowledge that he would establish and then call upon Special Operations Executive (SOE) and London Controlling Section (LCS). "It was Churchill

who had all of the ideas. It was his drive, his brilliant imagination, and his technical knowledge that initiated all these ideas and plans." [Brown, 1975, p. 8]

The SOE and LCS had special liaisons that worked effectively and efficiently with United States and their Office of Strategic Services (OSS). This sharing of information was key in the ramping up of U.S. intelligence operations, ensuring that their impact was quick, efficient and effective.

During the War, London became the center of anti-German Intelligence activities. Allied intelligence networks made London their center of operations. All European campaigns were directed from the London headquarters, as important information was gathered, analyzed and disseminated throughout Europe and around the globe.

1. London Controlling Section

London Controlling Section (LCS) was an organization established by Prime Minister Winston Churchill in 1941. LCS worked in cooperation with MI-5 (British security service responsible for domestic national security matters), MI-6 (British security service, otherwise known as the SIS, responsible for collecting foreign intelligence relating to national security), SOE and the OSS. The purpose of the LCS was to spread disinformation and coordinate all Allied deception efforts against the Axis.

Prior to World War II, British deception had been the responsibility of the Inter-Services Security Board (ISSB). In late 1940, the British North Africa campaign developed a special section of intelligence assets whose responsibility was to deceive the opposing Italian forces. It was the success of this deception, on a small scale, that led to

the establishment of LCS. London Controlling Section proved its' value during the landings of Sicily and Italy in 1943. LCS coordinated all information regarding the operation, spreading disinformation and gathering accurate information on enemy forces. The end result was a success, with Axis forces sparsely deployed along coastlines between Greece and Sardinia, posing a minimal threat to Allied forces.

In 1944 the Allies began preparations for invading Europe. Operation Bodyguard was commenced; a deception intended to conceal Allied intentions in northwest Europe. "[LCS] coordinated all British military, political, and civil agencies to make certain that they conformed to the multitude, of Bodyguard deception schemes." [Breuer, 1993] Coordination efforts were massive and detailed. The United States was a part of the deception with all efforts coordinated through the Joint Security Control (JSC). The JSC was the American version of the LCS with members from the Army, Navy and Air Corps.

The LCS employed many "soft" perception techniques, but when physical action was required they called upon MI-5, MI-6, SOE and the OSS. MI-5 worked with the Twenty Committee, other wise known as XX or Double Cross, and developed the deception plans for Normandy and coordinated all operations through the LCS. MI-5 and Scotland Yard aided the Double Cross Committee in capturing German agents that had infiltrated Britain. The XX Committee then turned the captured into double agents as to manipulate information received by German High Command. "It is essential to seek out enemy agents who have come to conduct espionage against you and to bribe them to serve you." [Sun Tzu, 1963, p. 148]

The cornerstone of secure German messages was the "Enigma." A revolutionary device that the German's thought was unbreakable. The British, via Ultra, used a captured German "Enigma" device to decode and encode Nazi message traffic. The XX Committee and Ultra provided LCS with the ability to coordinate information that was being pumped in to the Nazi information network (via XX), verify that the information had been received (via Ultra) and then confirm any Nazi reactions (via Ultra).

2. Special Operations Executive

Headquartered in London, Special Operations Executive (SOE) was established in July of 1940 by direction of Prime Minister Winston Churchill. The purpose of SOE was to coordinate all actions against the Axis by way of subversion and sabotage. In essence, SOE was a physical arm of London Controlling Section.

British Espionage efforts were crippled during the initial stages of the war. MI-6's intelligence networks were nearly completely compromised or destroyed. The SOE then began the rebuilding of these networks drawing assets from all sections of the British government. The SOE was divided into three sections; SO1 – Propaganda, SO2 – Active Operations, and SO3 – Planning.

The SOE took on activities previously carried out by the War Department's Military Intelligence Research (MI(R)), Section D of the Secret Intelligence Service or MI-6, and the Department of Propaganda of the Foreign Office or Department Electra House. The SOE was then empowered with coordinating all "subversive" plans. The SOE ensured that all irregular operations were in sync with general strategic plans.

Since organized resistance groups already existed in the Nazi occupied countries, the SOE was tasked with financing, supplying, and directing the different guerilla operations. SOE agents were assigned to the resistance groups, parachuting behind enemy lines. These agents were experts in espionage, electronics, explosives, and communications. SOE efforts used state-of-the-art technology and irregular tactics to disrupt communications, transportation and supply lines. Instrumental in the success of the D-Day Allied landings, the SOE was a key factor in stimulating resistance movements throughout Europe allowing the Allied forces to gain a foothold on the continent.

In 1946, after a nearly six-year battle against the Axis and their troops, the SOE was disbanded. It is impossible to list all of the SOE operations; many are still classified, even today. It is evident that the efforts of the SOE were vital to an Allied victory.

B. GERMAN INTELLIGENCE

In 1938 the Oberkommando der Wehrmacht (OKW) or High Command of the Armed Forces was established. The OKW replaced the old Reich War Ministry. The OKW coordinated all efforts of the German military forces.

Nazi Germany employed numerous intelligence agencies. The agencies included the Abwehr, the Sicherheitsdienst (Security Police), the Schutzstaffel (Protective Squadrons), the Reich Sicherheits Hauptamt (Main Security Office), and the Geheimes Staatspolizeiamt (Gestapo). The inherent problem of these agencies was that they not only conducted operations against the adversaries of Germany and the Nazi party, but against each other as well. The agencies became the personal troops of their respective

directors and were employed as political tools. None was more evident than the turmoil between The Abwehr's "old school" Wilhelm Canaris and the Sicherheitsdienst's "young devoted" Walther Schellenberg.

The two heads of Germany's intelligence agencies were mortal enemies. Canaris was an old school German who did not like what Hitler and the Nazi party had done to his homeland. On the surface, Canaris was an outspoken true believer in the Nazi cause. Underneath, Canaris was a traitor to the Nazi party who divulged secrets to the Allies and plotted a coup to assassinate Hitler. Schellenberg was a "genuine" true believer and had suspected that Canaris was a traitor, which is why the Sicherheitsdienst spied on the Abwehr.

1. The Abwehr & Brandenbourg Commandos

The Abwehr was Germany's foreign information and counterintelligence department. Established in 1866 as a Prussian agency, the Abwehr successfully conducted espionage against Austria in a conflict between the two Germanic nations. The Abwehr continued to prove itself in the Franco-Prussian War and World War I. After Germany's loss in WWI, the Abwehr was disbanded. Only to be reinstated in the early 1920's under the Weimar Republic.

The Abwehr was the German War Ministry's intelligence and espionage agency that was established in the early 1920's under the Weimar Republic. The Abwehr employed saboteur tactics by operating behind enemy lines just ahead of German forces. Utilizing a battalion of agents, the Abwehr would capture roadways, bridges, and other

strategically valuable targets before retreating forces could destroy them. This battalion of operatives was known as the "Ebbinghaus" battalion and was later renamed the "Brandenburg Commandos." The operatives that made up this special battalion were fluent in a number of different languages to include, Russian, Polish, Czech, and etc., which allowed them to infiltrate the variety operational areas.

2. The Sicherheitsdienst

The Sicherheitsdienst (SD), or "Security Police", was the political intelligence arm of the Schutzstaffel (SS) or "Protective Squadrons". The mission of the SD was to conduct intelligence operations for the German state and the Nazi party. The SD was tasked with obtaining secret information on current and potential enemies of the state or the party, so that those threats could be neutralized. Unfortunately, a few of the current and potential enemies of the Nazi party were internal high-ranking members.

C. INFORMATION: THE DECISIVE FACTOR

The continuity between agencies and their ability to share information, work together and combine assets made the difference. "...the SD and Abwehr were devoting more energy and time in trying to discredit one another than they were spending in seeking to unlock the secrets of the looming assault on Fortress Europe." [Breuer, 1993, p.19] The arrogance of the Nazi's in declaring their "enigma" unbreakable left them complacent and vulnerable. The Allies were able to compromise the German information network, pump in disinformation and get feedback without them even knowing.

During the Battle of Britain, it was the ability of Ultra combined with the use of radar and human spotters that produced excellent information on the location of incoming German bombers. The Royal Air Force (RAF) was then waiting to prey upon the unsuspecting bombers. To protect their access to the German information, the British would first send a scout plane and/or fake a radio transmission spotting the incoming bombers. This was done so that the Germans would not suspect a leak in their information network. This represents the effective blending of technology and "soft" perception techniques to achieve a decisive advantage in Information Operations.

D. BRINGING IO FORWARD

The authors believe, that the abilities displayed by the British and the Allies in gaining "information superiority" are exactly what must be emulated. Although today's conflicts are not to the scale of World War II, there are still those who would do harm to the United States. The technology today allows the smallest of groups, not even a nation state, to inflict significant amounts of damage. Attacks may range from weapons of mass destruction (WMD) to a distributed denial of service (DDOS) network attack. In all cases information is at the center. Aggressive IO may uncover a plot to detonate a nuclear weapon inside the continental U.S. and solid IO defense measures may defuse a harmful computer virus before it infects millions of computers. Information Operations must be attended to, from both a technology and a "soft" perspective.

III. OVERVIEW OF PRESENT INFORMATION OPERATIONS

A. PURPOSE

The purpose of this chapter is to establish a common understanding through terminology and concepts. A description of the current IO organization will depict who the main players are within each executive agency and how they interact. In today's environment the private sector has taken the lead in terms of technological innovation and organizational practice. The Chief Information Officer (CIO) of a large corporation today, is a key figure of the organization. The CIO works closely with the Chief Executive Officer (CEO) in developing strategy, policy, milestones and goals. The CIO oversees, all aspects of information, from information systems to public relations. The government has adopted many of the new technologies used in the private sector. The authors suggest that the government must now take a few pages from of the private sector's organizational playbook.

B. ART VS. SCIENCE

Information Operations (IO) integrates areas such as electronic warfare (EW), psychological operations (PSYOPs), public affairs (PA), information security (IS), civil affairs (CA). In effect IO has blended the two polarized sides of information management and information manipulation; art and science.

The art side incorporates diplomacy, public affairs (PA), civil affairs (CA), psychological operations (PSYOPs), deception and some aspects of operational security (OPSEC) into the larger picture of IO. These forms of IO require the employment of "soft" perception techniques that attack, defend and exploit the inner workings of the human mind and cultures. These "soft" techniques are aimed at influencing a target audience, whether it is a small group or an entire population.

The science side involves technology in the forms of computer network attacks (CNA), computer network defense (CND), cyber-terrorism, physical destruction, electronic warfare (EW) and such. The science side of IO depicts an offensive advantage, in that anyone with the equipment and the savvy may conduct a CNA in the form of a distributed denial of service (DDOS) attack or computer virus. As quickly as defensive measures are taken, they are unable to keep up. [Gerblick, 2000, p. 3]

C. THE CHIEF INFORMATION OFFICER'S COUNCIL

The Chief Information Officers (CIO) Council was established by Executive Order 13011, Federal Information Technology, on July 16, 1996 (APPENDIX E. EXECUTIVE ORDER 13011 OF JULY 16, 1996). This was later named the Clinger-Cohen Act. The CIO Council serves as the principal inter-agency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. The Council's role includes developing recommendations for information technology management (ITM) policies, procedures,

and standards; identifying opportunities to share information resources; and assessing and addressing the needs of the Federal Government's IT workforce. [cio.gov]

The Chair of the CIO Council is the Deputy Director for Management for the Office of Management and Budget (OMB) and the CIO Council elects the Vice Chair from its membership. Membership on the Council is comprised of CIOs and Deputy CIOs from the Federal executive agencies:

Department of State	Department of the Treasury	Department of Defense
Department of Justice	Department of the Interior	Department of Agriculture
Department of Commerce	Department of Labor	Department of Health and Human Services
Department of Housing and Urban Development	Department of Transportation	Department of Energy
Department of Education	Department of Veterans Affairs	Environmental Protection Agency
Federal Emergency Management Agency	Central Intelligence Agency	Small Business Administration
Social Security Administration	National Aeronautics and Space Administration	Agency for International Development
General Services Administration	National Science Foundation	Nuclear Regulatory Commission
Office of Personnel Management		

Table 2. Members of the CIO Council

CIO Council membership may also include representatives from the smaller Federal agencies, and liaisons to other executive councils, committees, and boards.

The CIO Council serves as a focal point for coordinating inter-agency challenges. The CIO Council committees are designated to meet these challenges. The Council's committees for the year 2000 included: Capital Planning and IT Management; Federal IT

Workforce; Security, Privacy and Critical Infrastructure; Enterprise Interoperability and Emerging IT; Outreach; and E-Gov.

D. EXECUTIVE AGENCY ORGANIZATIONS

1. Department of Defense

The mission of the Department of Defense is to provide the military forces needed to deter war and to protect the security of the country.

The Department of Defense is divided into several groups: three military departments, fourteen defense agencies, nine field activities, nine Unified Combatant Commands, the Joint Chiefs of Staff (JCS), the Inspector General (IG) and the Office of the Secretary of Defense (OSD).

The military departments include the Army, the Air Force and the Navy-Marne Corps. These departments are responsible for recruiting, training and equipping their forces, but operational control of those forces is assigned to one of the unified combatant commands. [defenselink.mil]

The fourteen defense agencies include:

Ballistic Missile Defense Organization	Defense Advanced Research Projects Agency	Defense Commissary Agency
Defense Contract Audit Agency	Defense Finance and Accounting Service	Defense Information Systems Agency
Defense Intelligence Agency	Defense Legal Services Agency	Defense Logistics Agency
Defense Security Cooperation Agency	Defense Security Service	Defense Threat Reduction Agency
National Imagery And Mapping Agency	National Security Agency	

Table 3. Defense Agencies

The nine Unified Combatant Commands are:

U.S. European Command	U.S. Pacific Command	U.S. Joint Forces Command
U.S. Southern Command	U.S. Central Command	U.S. Space Command
U.S. Special Operations Command	U.S. Transportation Command	U.S. Strategic Command

Table 4. Unified Combatant Commands

The nine Field Activities are:

American Forces Information Service	Defense Prisoner of War/Missing Personnel Office	DoD Human Resources Activity
DoD Education Activity	Defense Medical Programs Activity	Office of Economic Adjustment
Washington Headquarters Services	Office of Civilian Health & Medical Program of the Uniformed Services	Defense Technology Security Administration

Table 5. Field Activities of the DOD

The Office of the Secretary of Defense (OSD) is responsible for the development of policy, planning, resource management, finances, and program evaluation. OSD includes the immediate offices of the Secretary and Deputy Secretary of Defense, Under

Secretaries of Defense, Director of Defense Research and Engineering, Assistant Secretaries of Defense, General Counsel, Director of Operational Test and Evaluation, Assistant Secretary of Defense (ASD) - Command, Control, Communications, and Intelligence (C3I), Assistant Secretary of Defense Legislative Affairs, Assistant Secretary of Defense Public Affairs, and Director of Administration and Management. The entire DoD Organization is depicted in Figure 1.

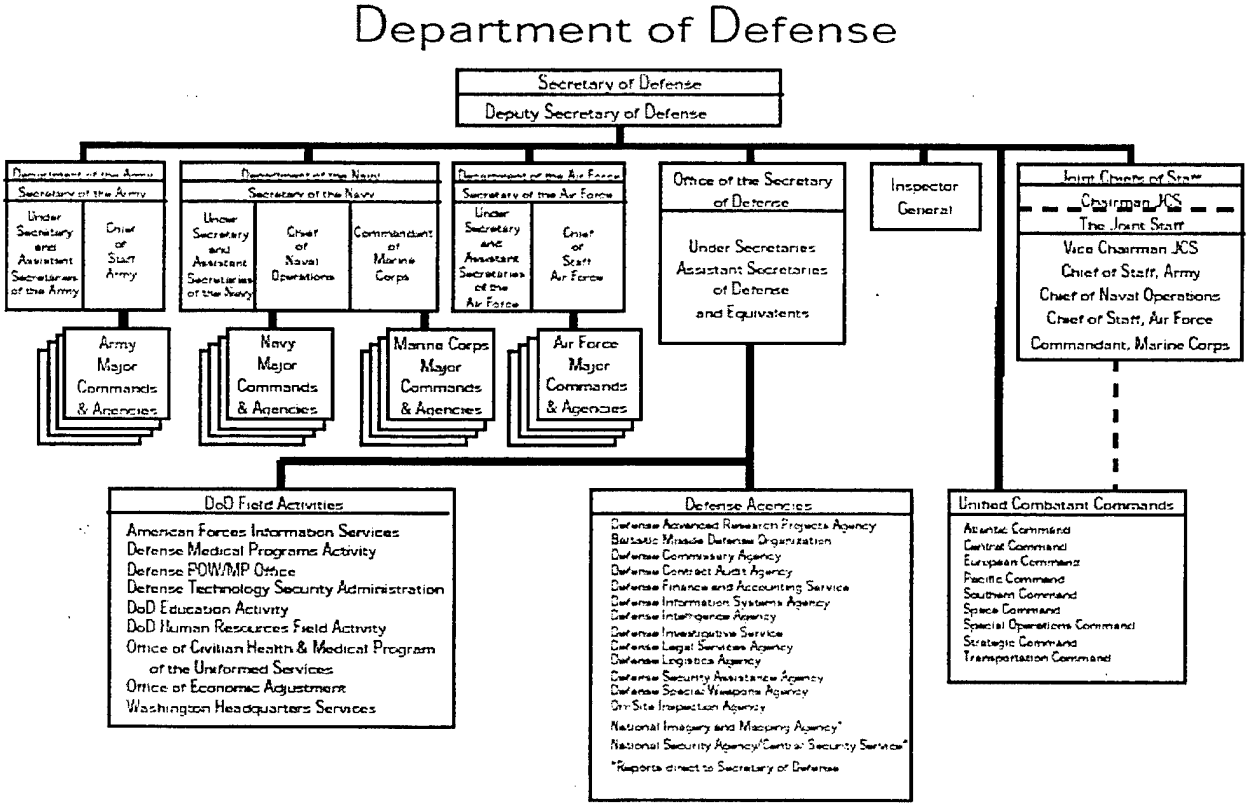

Figure 1. DoD Organizational Chart (as of Dec 2000) [From: defenselink.mil]

The Secretary's primary subordinate responsible for Information Operations (IO) is the Chief Information Officer (CIO). The ASD-C3I performs the duties of CIO. The ASD-C3I has four Deputies: Deputy CIO; Intelligence; Security & Information Operations; Command, Control, Communications, Intelligence, Surveillance, Reconnaissance (C3ISR) & Space; Program & Evaluation. The CIO's Organization is represented in Figure 2.

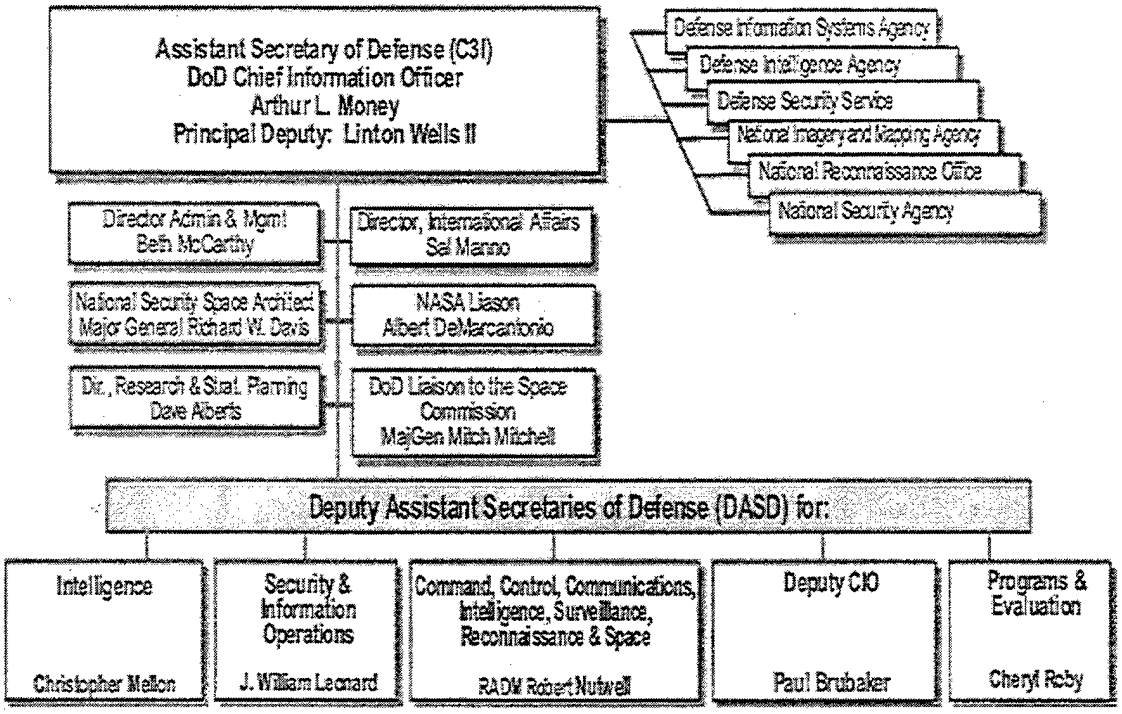

Figure 2. DoD CIO Organizational Chart (as of Jan 2001) [From: defenselink.mil]

2. Department of State

The State Department is the lead agency on matters regarding foreign affairs. The department advances U.S. objectives and interests abroad by formulating, representing, and implementing the President's foreign policies. Major agencies within the department include the Arms Control and Disarmament Agency (ACDA), the Agency for International Development (USAID) and the Office of International Information Programs, all of which are subordinate to the Secretary of State. [state.gov]

The State Department is headed by the Secretary of State. The secretary is aided by a Deputy Secretary, five Under Secretaries (Political Affairs; Economic, Business and Agricultural Affairs; Arms Control and International Affairs; Management; and Global Affairs) and 19 Assistant Secretaries. The Assistant Secretaries are responsible for the numerous functions that make up the State Department. (See Figure 3.) Their responsibilities are broken up by region and/or areas of specialty. There are numerous additional assistants and specialists that are employed to maintain an effective grasp of the world's international relations. One of these assistants/specialists is the Chief Information Officer (CIO).

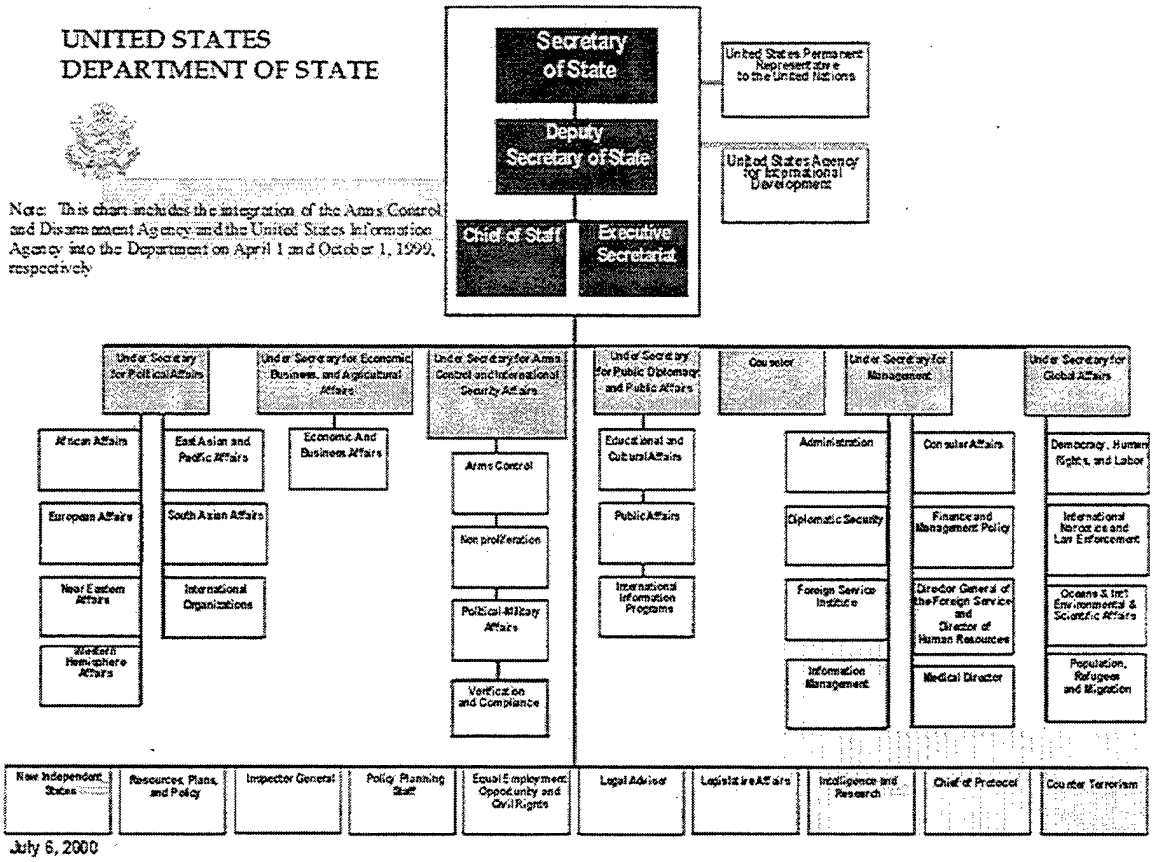

Figure 3. DOS Organizational Chart (as of Oct 1999) [From: state.gov]

The CIO is the Department's lead official responsible for the information technology (IT) operations, policies and plans needed to achieve strategic Department missions. The CIO is the equivalent of an assistant secretary, and serves as the Under Secretary for Management's principal advisor on IT matters. The CIO also heads the Department's Bureau of Information Resource Management (IRM). The IRM Bureau's mission is to provide the Department of State the reliable, secure, and high quality IT infrastructure and services that are fundamental to foreign affairs operations and the conduct of U.S. diplomacy. The CIO is supported by four primary deputies: Operations;

Architecture, Planning and Regulations; Management and Customer Service and Foreign Affairs System Integration. (See Figure 4.)

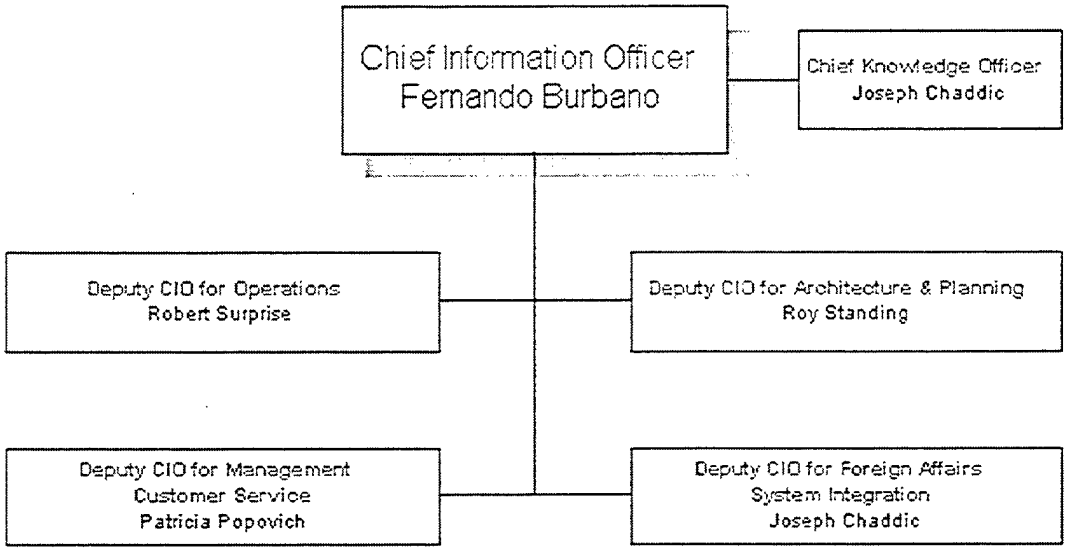

Figure 4. DOS CIO Organizational Chart (as of Jan 2001) [From: state.gov]

3. Department of Justice

The Department represents the citizens of the United States in enforcing the law in the public interest and plays a key role in protection against criminals; ensuring healthy competition of business; safeguarding the consumer; enforcing drug, immigration, and naturalization laws; and protecting citizens through effective law enforcement. The Department conducts all suits in the Supreme Court in which the United States is concerned. It represents the Government in legal matters rendering legal advice and opinions, upon request, to the President and to the heads of the executive departments.

The affairs and activities of the Department are supervised and directed by the Attorney General (AG). [usdoj.gov]

The AG directs and oversees the work of more than 30 separate component organizations of the Department. (See Figure 5.) These components include the Department's five major law enforcement bureaus: the Federal Bureau of Investigation (FBI); the Drug Enforcement Administration (DEA); the United States Marshals Service (USMS); the Immigration and Naturalization Service (INS); and the Bureau of Prisons (BOP). There are also six divisions that conduct litigation (Civil, Criminal, Antitrust, Civil Rights, Environment and Natural Resources, and Tax), the U.S. Attorneys, and a number of additional organizations (offices and boards) essential to the Department's fulfillment of its mission.

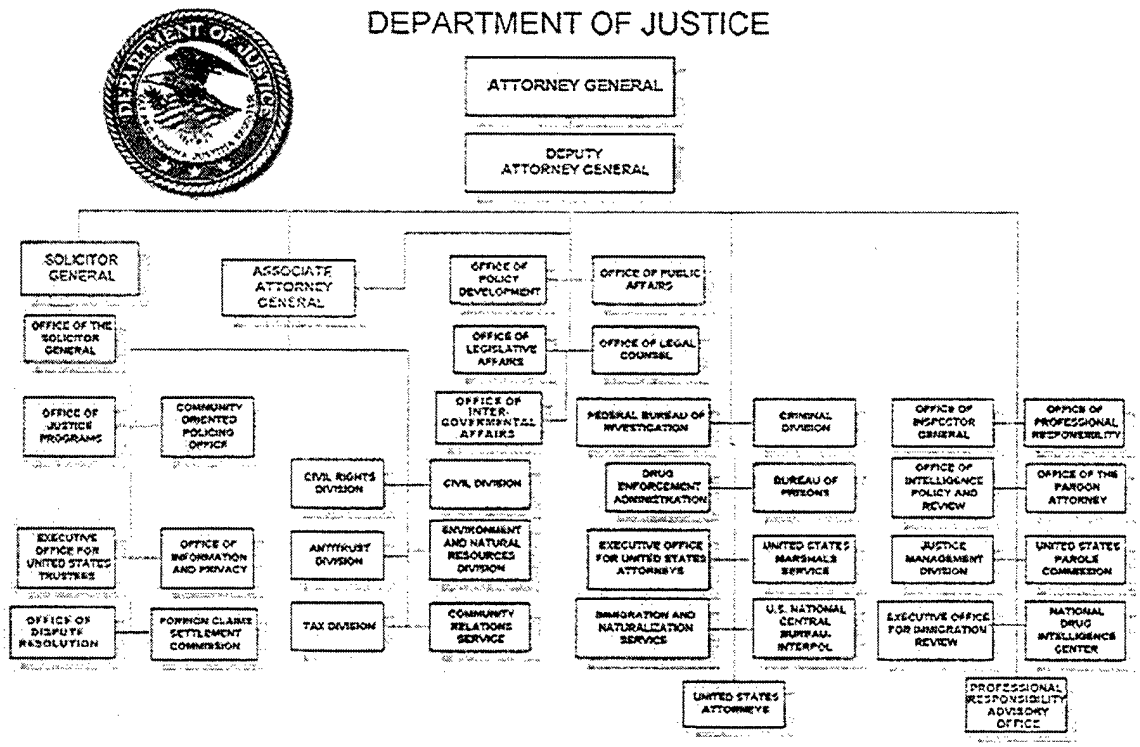

Figure 5. DOJ Organizational Chart (as of Feb 2001) [From: usdoj.gov]

The Assistant Attorney General for Administration (AAG/A) heads the Justice Management Division (JMD) and serves as the Department's Chief Information Officer (CIO). The JMD is the principal administrative arm of the Department. The JMD controls policy, oversight, and service delivery responsibilities in such diverse functional areas as budget, finance, procurement, personnel, and the Information Resources Management (IRM) staff. The CIO or AAG/A is supported by four key deputies: IRM; Controller; Human Resources/Administration; and Law & Policy. (See Figure 6.)

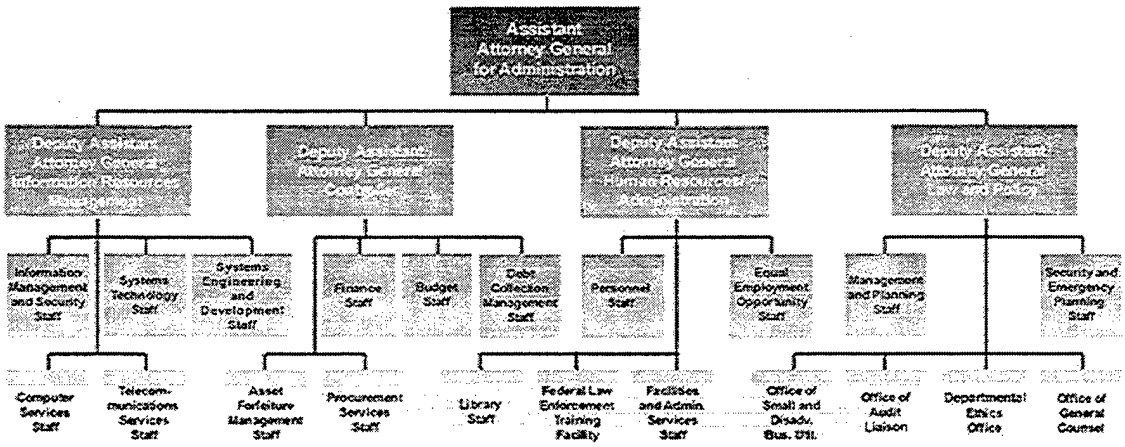

Figure 6. DOJ CIO Organizational Chart (as of Jan 2001) [From: usdoj.gov]

4. Department of Commerce

The Department of Commerce (DOC) promotes job creation, economic growth, sustainable development and improved living standards for all Americans by working in partnership with business, universities, communities and workers. The DOC promotes U.S. competitiveness in the global marketplace by strengthening and safeguarding the nation's economic infrastructure. U.S. Industry is kept competitive with cutting-edge science and technology and an unrivaled information base. The DOC manages the nation's resources and assets to ensure sustainable economic opportunities. [doc.gov]

The Department is broken down into ten offices:

Bureau of Export Administration (BXA)	Economics & Statistics Administration (ESA)	Economic Development Administration (EDA)
International Trade Administration (ITA)	National Oceanic & Atmospheric Administration (NOAA)	Minority Business Development Agency (MBDA)
National Telecommunications & Information Administration (NTIA)	Office of the Inspector General (IG)	Patent & Trademark Office (PTO)
Technology Administration (TA)		

Table 6. Offices of the DOC

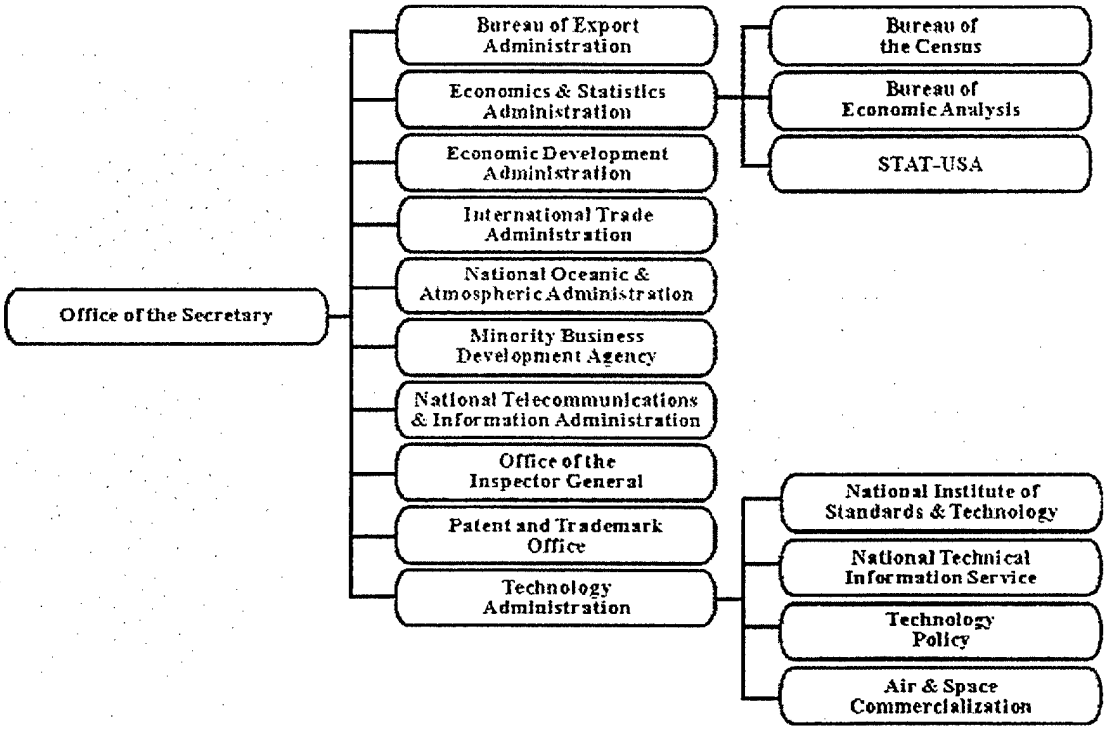

Figure 7. DOC Organizational Chart (as of Dec 2000) [From: doc.gov]

The DOC has taken the approach of creating an independent position of CIO. The role of the DOC CIO is to provide guidance to the CIOs of all the Bureaus and Operating Units within the DOC. In addition, the DOC CIO manages Programs such as Digital

Department, Y2K requirements compliance, Protection of the Critical Infrastructure, and Data Center consolidation, which are most effectively run on a centralized basis. The DOC CIO advises the Secretary on all matters regarding IT.

The bureau CIOs manage the IT within their bureaus, coordinating with the DOC CIO. CIOs of the Operating Units within the bureau manage the IT within their Operating Units and coordinate with the bureau CIO on IT activities within their Units. All DOC bureau CIOs are to attend the DOC CIO Council Meetings. At these meetings, the bureau CIOs exchange ideas and provide the DOC CIO with inputs on Department policy and procedures.

The DOC CIO has eight internal offices that support him/her:

Digital Department	Office of Computer Services (OCS)	Office of Information Collection and Analysis (OICA)
Office of Information Planning and Review (OIPR)	Office of Information Policy and Technology (OIPT)	Office of Information Systems (OIS)
Office of Technical Support and Network Services (OTS&NS);	Office of Telecommunications Management (OTM)	

Table 7. Offices of the DOC CIO

The Digital Department is responsible for planning and coordinating activities necessary for Commerce to perform most internal and external processes electronically.

The Office of Computer Services (OCS) manages and operates a computer center to support the Office of the Secretary and designated operating units. The Office of Information Collection and Analysis administers the Paperwork Reduction Act (PRA).

The Office develops Department-wide policy and guidance for the program and provides ongoing assistance to Commerce operating units in implementing the PRA. The Office reports to the Director for Digital Department.

The OIPR administers the IT planning, IT investment review, computer security, and IT architecture and standards programs. OIPR develops Department-wide policy and guidance for all four programs and provides ongoing assistance to Commerce operating units in implementing these programs.

The OIPT administers the CIO's information technology risk management program, the IT liaison program to the operating units and coordinates IT data calls from OMB and other Federal departments. OIPT develops Departmental policy for management and use of IT resources, as well as the acquisition of these resources. OIPT also recommends approval or disapproval to the CIO for requirements initiative/business case justification, specifications and benefit/cost analyses for IT resources from the operating units.

The OIS reports to the Digital Department Director. OIS provides systems analysis, design, development support, and oversight for Department automated systems for administrative and program management (excluding financial systems). OIS develops and manages numerous administrative and management systems in support of the Department's program offices.

The OTS&NS provides a broad range of technical and systems management assistance for the Secretary and designated operating units.

The OTM reports to the Digital Department Director. OTM develops and implements policies and guidelines related to Commerce telecommunications and coordinate the management of all Departmental telecommunication systems

5. Department of the Treasury

The Mission of the Department of the Treasury is to, promote prosperous and stable American and World economies, manage the Government's Finances, safeguard all Financial Systems, protect the nation's leaders, and secure a safe and drug-free environment. [treasury.gov]

The Department is made up of numerous offices, bureaus and services to include:

Departmental Offices	Office of Inspector General (IG)	Internal Revenue Service (IRS)
U.S. Customs Service (USCS)	Bureau of Alcohol, Tobacco & Firearms (ATF)	U.S. Secret Service (USSS)
Federal Law Enforcement Training Center (FLETC)	Financial Crimes Enforcement Network (FinCEN)	Treasury Forfeiture Fund (TFF)
Office of the Comptroller of the Currency (OCC)	Office of Thrift Supervision (OTS)	U.S. Mint
Bureau of Engraving and Printing (BEP)	Financial Management Service (FMS)	Bureau of the Public Debt (BPD)
Community Development Financial Institutions (CDFI) Fund	Treasury Inspector General for Tax Administration	

Table 8. Offices of the Treasury

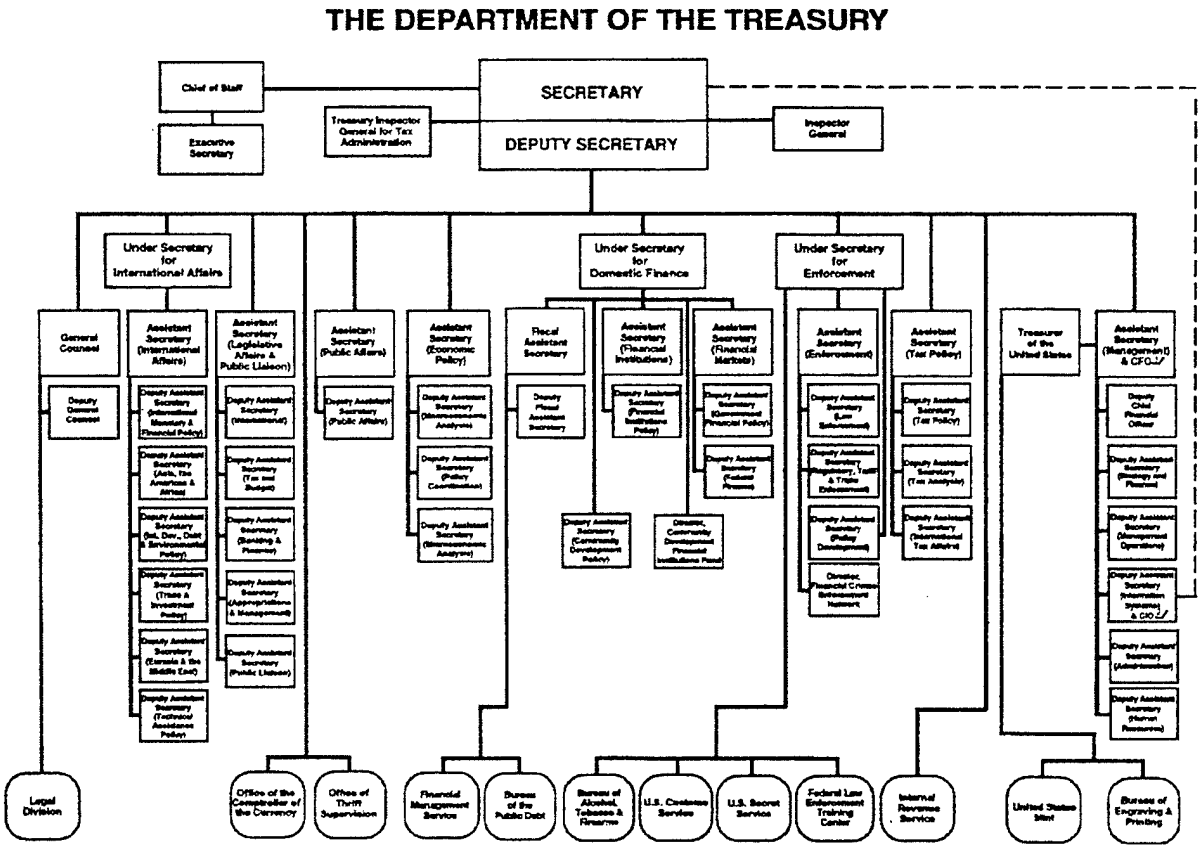

Figure 8. Treasury Organizational Chart (as of Nov 2000) [From: treasury.gov]

The Deputy Assistant Secretary Information Systems (DASIS) is the CIO of the Treasury Department. Treasury has approached the task of IO in a way congruent to that of the DOC. Although they have added a title to an existing position, the DASIS, the Treasury has established a CIO for each bureau, office and service. Each of those CIOs is subordinate to the DASIS on issues regarding IT. The office of the CIO is divided into seven sections: Senior Technical Officer (STO); Administrative Support; Security; IT Policy and Strategy; Infrastructure and Operations; Customer Service Consulting; and Chief Operating Officer (COO)/ Business Practices. (See Figure 9.)

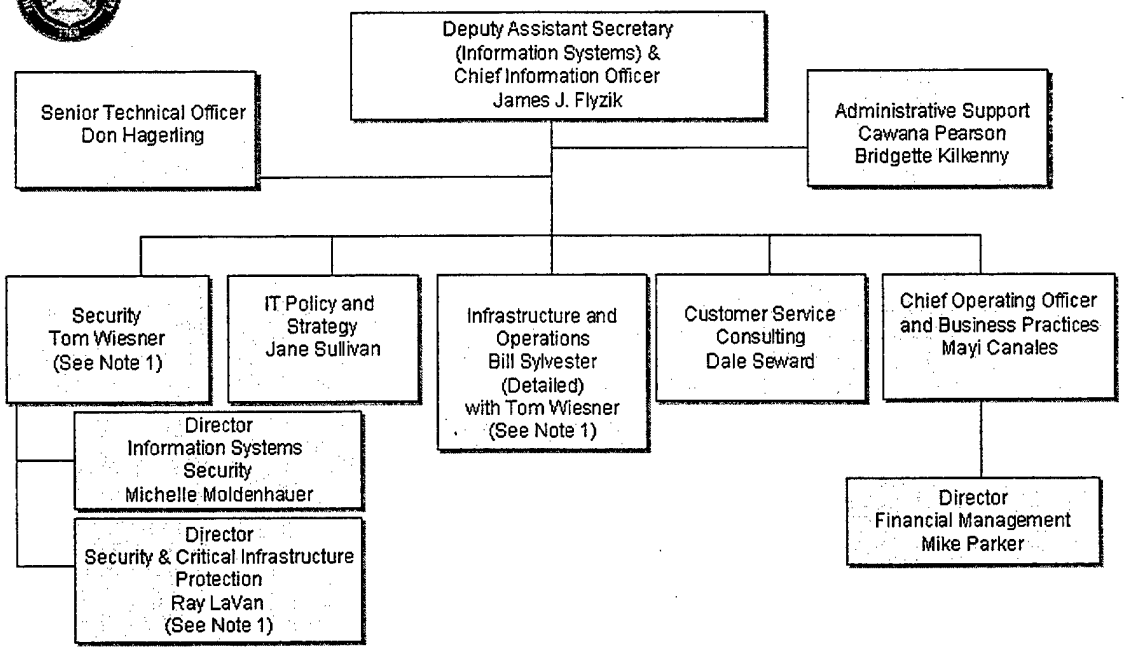

Figure 9. Treasury CIO Organizational Chart (as of Jan 2001) [From: treasury.gov]

6. Department of Energy

The Department of Energy's (DOE) mission is provide a secure and reliable energy system that is environmentally and economically sustainable, to oversee the Nation's nuclear programs, and to ensure the United States remains on the cutting edge of science and technology. [energy.gov]

The DOE is comprised of over 31 offices broken up into 3 key groups: the Under Secretary of Nuclear Security; the Under Secretary for Energy, Science and Environment, and the Departmental Staff and Support Offices. (See Figure 10.)

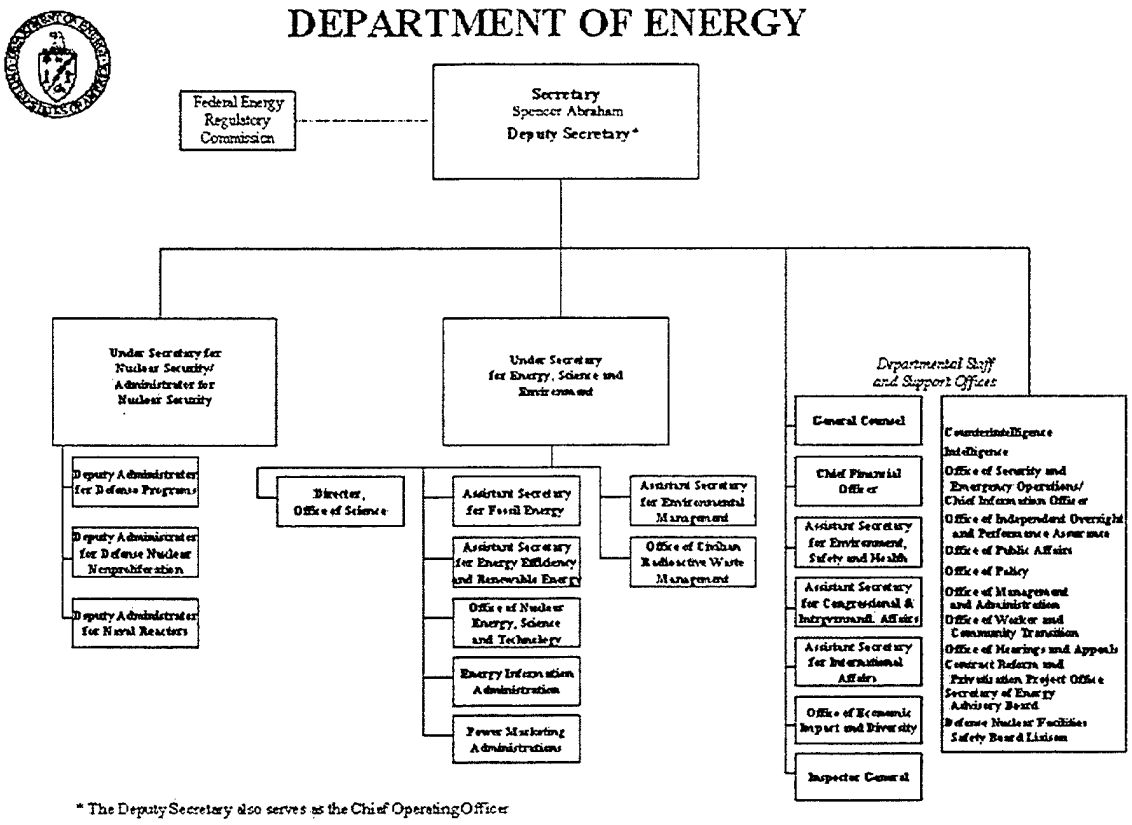

Figure 10. DOE Organizational Chart (as of Dec 2000) [From: energy.gov]

The Director of Security and Emergency Operations was designated the DOE's CIO. The CIO supports the Secretary on all departmental IT concerns. The CIO is supported by five offices: Records and Business Management; Architecture, Standards and Policy; Cyber Security; Operations; and Special Projects. (See Figure 11.)

The Office of Records, & Business Management ensures that the Department's recorded information is managed in an economical, effective, and efficient manner throughout its life cycle in support of mission accomplishment and accountability.

The Office of Architecture, Standards, and Policy provides advice and other assistance to the CIO and other senior management personnel to ensure that information technology and resources are planned for, acquired and managed in a manner that implements the policies and procedures of legislation.

The Office of Cyber Security manages the Department-wide communications security (COMSEC), Unclassified Computer Security programs, and provides assistance and guidance in these areas to all DOE entities.

The Office of Operations provides advice and technical infrastructure support to the CIO and other senior Departmental officials to ensure delivery of vital Information Management (IM) and Information Technology (IT) services.

The Special Projects Office identifies, directs, and manages high-priority corporate information management and information technology projects. This office also advises the CIO and Senior DOE Management on the implementation of information technology solutions to achieve management efficiencies in business processes.

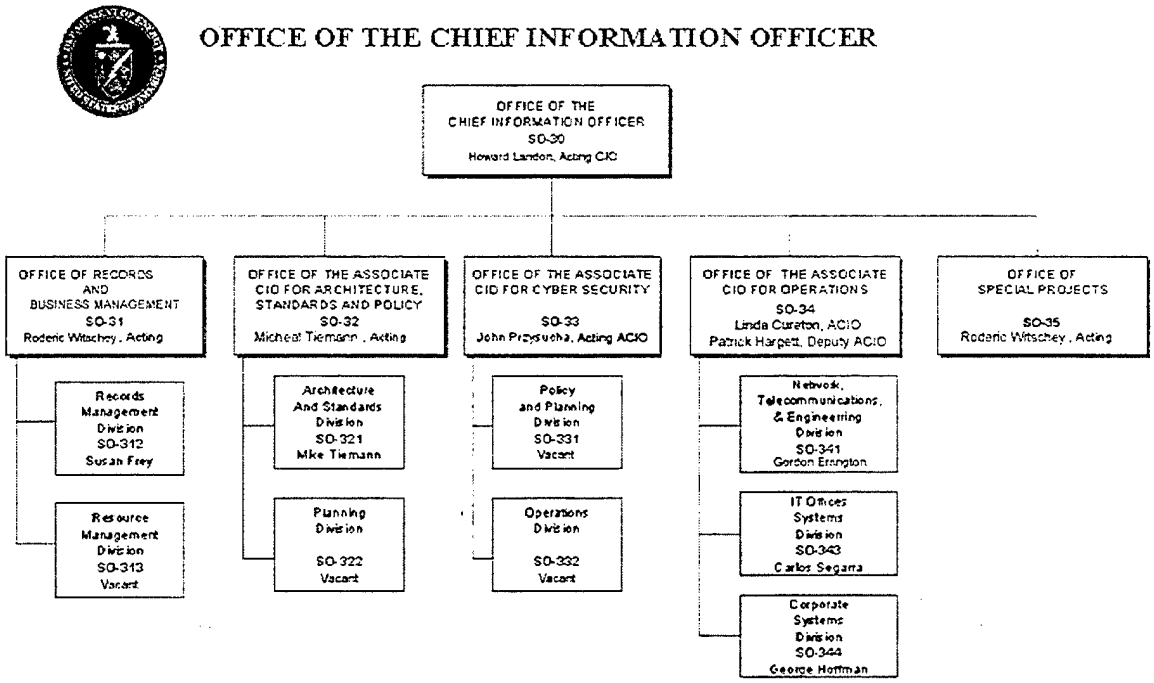

Figure 11. DOE CIO Organizational Chart (as of Dec 2000) [From: doe.gov]

7. Department of Transportation

The mission of the Department of Transportation (DOT) is to ensure that the U.S. has a fast, safe, efficient, accessible and convenient transportation system that meets vital national interests and enhances quality of life. [dot.gov]

The DOT is made up by a number of organizations. Key organizations include:

Office of the Secretary of Transportation (OST)	Bureau of Transportation Statistics (BTS)	Federal Aviation Administration (FAA)
Federal Highway Administration (FHWA)	Federal Motor Carrier Safety Administration (FMCSA)	Federal Railroad Administration (FRA)
Federal Transit Administration (FTA)	Maritime Administration (MARAD)	National Highway Traffic Safety Administration (NHTSA)
Office of the Inspector General (OIG)	Research and Special Programs Administration (RSPA)	Saint Lawrence Seaway Development Corporation (SLSDC)
Surface Transportation Board (STB);	Transportation Administrative Services Center (TASC)	United States Coast Guard (USCG)

Table 9. Organizations of the DOT

A full view of the DOT organization is depicted in Figure 12.

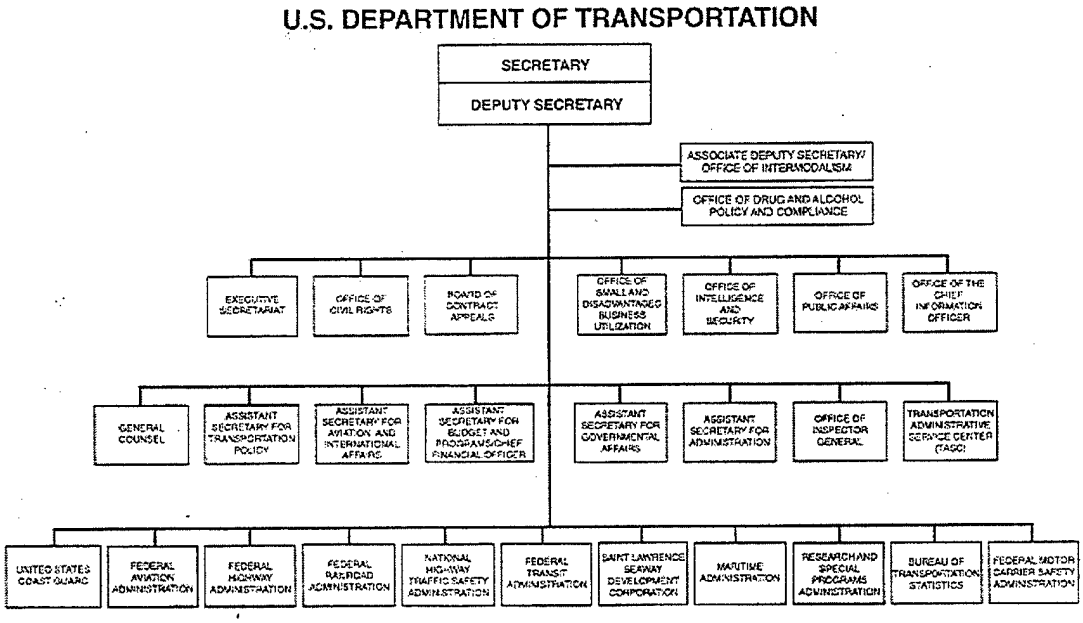

Figure 12. DOT Organizational Chart (as of Dec 2000) [From: dot.gov]

The DOT CIO is an independent entity that is responsible for all departmental IO. The DOT CIO chairs a Council that includes CIOs or senior IT officials from the thirteen operating entities within DOT. Additional members include representatives from the CFO, Inspector General and General Counsel's offices. The DOT CIO is supported by a structure consisting of Strategic Planning and Policy, IT Security, Enterprise Architecture (EA), Capital Planning and Investment Control (CPIC), Operations & Technology, E-government and Workforce Issues committees was established to bring focus on these priority Council areas. (See Figure 13.)

Strategic Planning and Policy Division ensures that all IT programs support the strategic goals and objectives of the Department. The division provides leadership and establishes policy to address regulatory requirements.

The Operations & Technology staff provides complete information technology support to all personnel within the Department.

The Enterprise Architecture defines the strategic information asset base which defines: the information necessary to operate the business, the technologies necessary to support the business operations, and the transitional processes necessary for implementing new technologies in response to a dynamic environment.

IT Security maintains the security of all IT systems vital to the mission of DOT. This office is responsible for the overall management and guidance of the Department's IT Security Program.

The overall goal of the Capital Planning And Investment Control (CPIC) office is to establish and maintain a Department-wide process that will use long-range strategic

planning and a disciplined budget process as the basis for efficient management of a portfolio of capital assets.

The E-Government Division is responsible for providing leadership throughout the DOT for the transition to digital government, including managing the departmental Internet and intranet web sites.

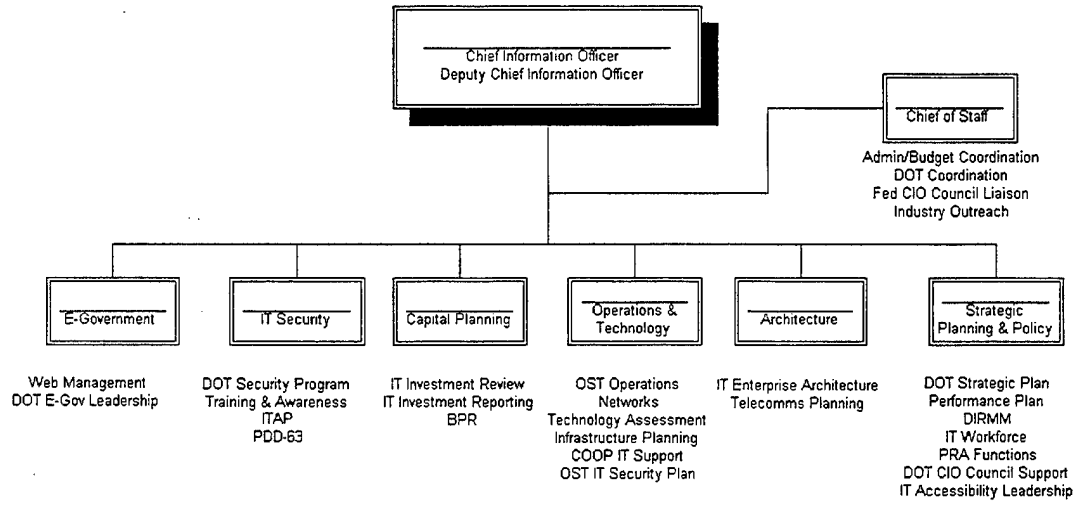

Figure 13. DOT CIO Organizational Chart (as of Dec 2000) [From: dot.gov]

8. Department of Agriculture

The mission of the United States Department of Agriculture (USDA) is to enhance quality of life by supporting the production of agriculture; ensuring a safe, affordable, nutritious, and accessible food supply; caring for agricultural, forest, and range lands; supporting sound development of rural communities; providing economic opportunities for farm and rural residents; expanding global markets for agricultural and

forest products and services and working to reduce hunger in the States and throughout the world. [usda.gov]

The Department is divided up into seven main agencies and offices headed by their respective Under Secretaries: Farm and Foreign Agriculture Services; Food, Nutrition and Consumer Services; Food Safety; Marketing and Regulatory Programs; Natural Resources and Environment; Research, Education, and Economics; and Rural Development. (See Figure 14.)

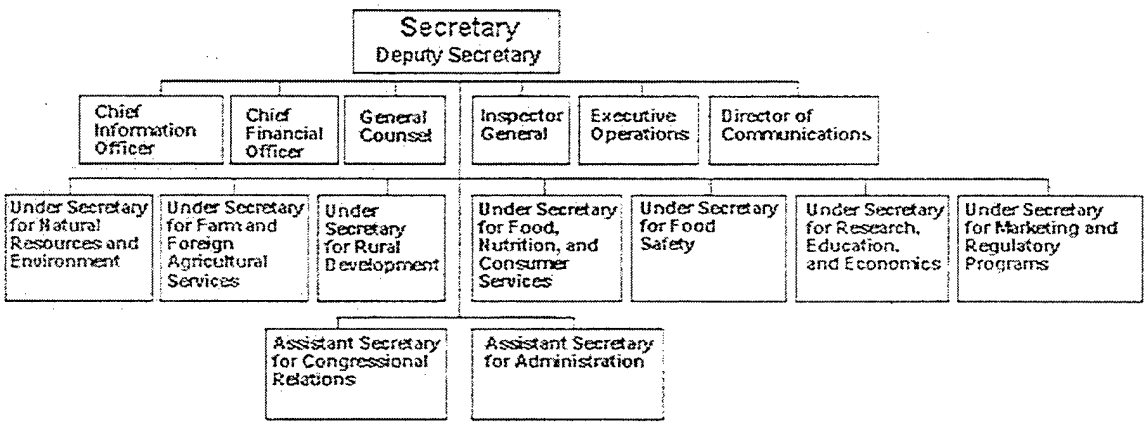

Figure 14. USDA Organizational Chart (as of Jan 2001) [From: usda.gov]

The USDA CIO is independent of any other office or agency of the Department. The CIO reports directly to the Secretary and has primary responsibility for supervision and coordination within the Department. The Office of the CIO supervises and coordinates the design, acquisition, maintenance, use, and disposition of IT by USDA agencies.

The Office of the CIO is dived up into three key sections: National Information Technology Center; Information Resources Management (IRM); and

Telecommunications Services & Operations. The CIO is also supported by the Resource Management Staff that provides leadership, consultation and support services in the management of resources. (See Figure 15.)

The National Information Technology Center participates with the CIO in the formulation, implementation, and evaluation of program development and delivery in the area of Technology Management (TM).

IRM is the Strategic information arm of the CIO. The IRM advises the CIO in the development of government-wide policies and initiatives in the application of IT to programs. This office also analyzes the impact of government-wide information management trends and develops appropriate USDA principles, policies, and standards.

The office of Telecommunications Services & Operations assists the CIO in the formulation, implementation, and evaluation of program development and delivery in the area of Telecommunications Services.

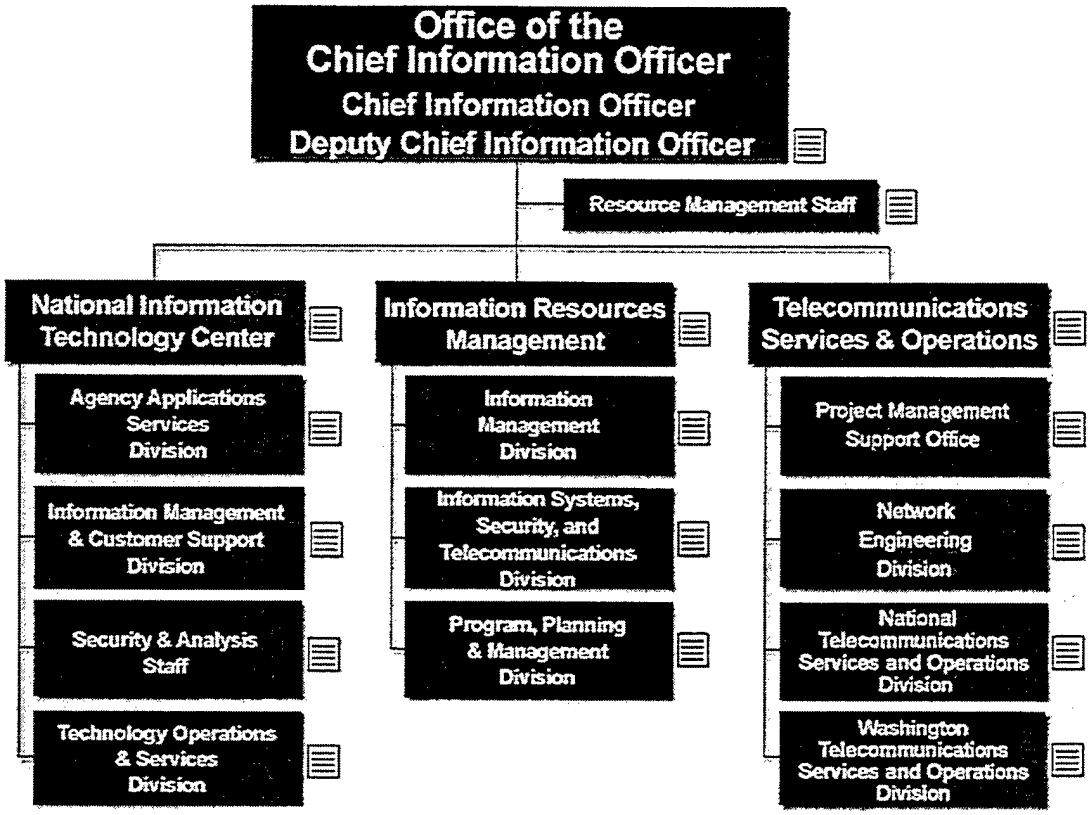

Figure 15. USDA CIO Organization Chart (as of Jan 2001) [From: usda.gov]

9. Department of Labor

The Mission of the Department of Labor (DOL) is to prepare the American workforce for new and better jobs, while ensuring the adequacy of America's workplaces. The DOL is responsible for the administration and enforcement of over 180 federal statutes supporting the protection of workers' wages, health and safety, employment and pension rights; equal employment opportunity; job training, unemployment insurance and workers' compensation programs.

The Department is separated into 18 sections:

Adjudicatory Agencies	Office of Small Business Programs (OSBP)	Occupational Safety & Health Administration (OSHA)
Employment & Training Administration (ETA)	Mine Safety and Health Administration (MSHA)	Pension & Welfare Benefits Administration (PWBA)
Veteran's Employment & Training Service (VETS)	Employment Standards Administration (ESA)	Bureau of Labor Statistics (BLS)
Women's Bureau (WB)	Bureau of International Labor Affairs (ILAB)	Office of Congressional and Intergovernmental Affairs
Office of the Assistant Secretary for Administration and Management (OASAM)	Office of the Assistant Secretary for Policy (OASP)	Office of the Chief Financial Officer (OCFO)
Office of the Solicitor (SOL)	Office of the Inspector General (IOG)	Office of Public Affairs (OPA)

Table 10. Offices of the DOL

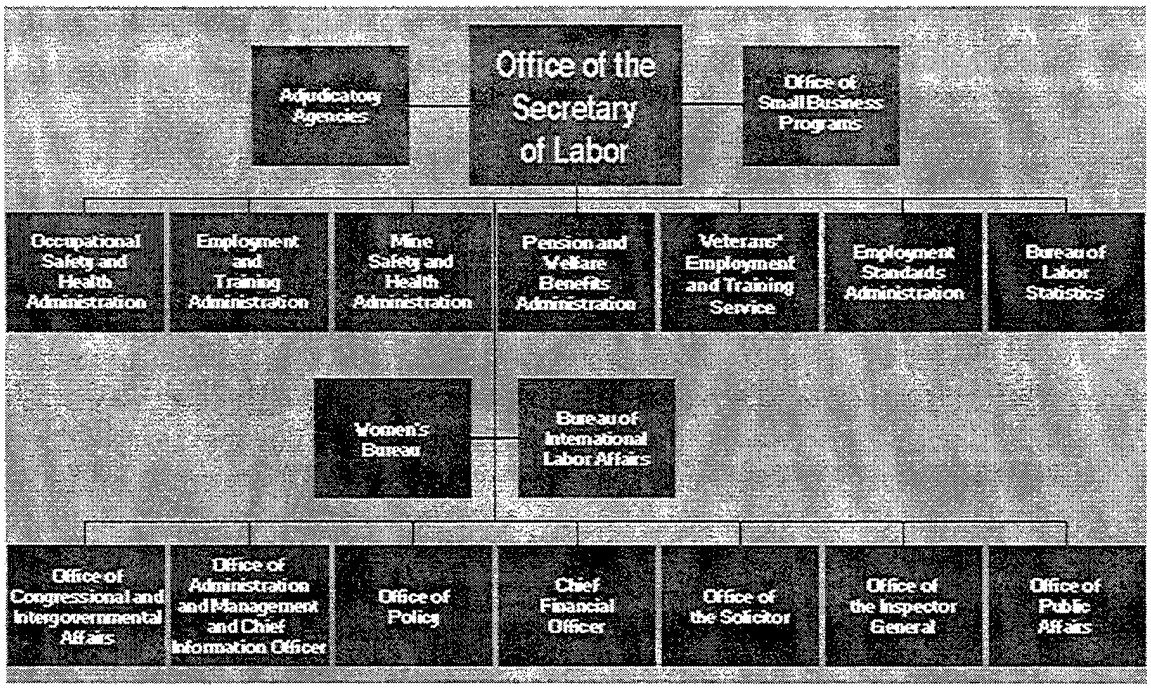

Figure 16. DOL Organizational Chart (as of Nov 2000) [From: dol.gov]

The Assistant Secretary of Administration and Management is the departmental CIO. The CIO is tasked with harnessing the power of modern IT to enable the efficient and effective delivery of Department of Labor services to external and internal customers. The CIO provides leadership, policy guidance and assistance to Departmental agencies in all aspects of using information technology to implement and manage those programs within the Department.

Although the CIO has not yet established an organizational hierarchy the following boards and teams are in affect: The Capital Planning and Investment Board (CPIB); the Computer Security group; and the IT Architecture team. The OCIO has also established policies and set forth a strategic plan.

The CPIB ensures that the departmental information system investments are based upon decision criteria which take into consideration risk- adjusted return and emphasize interoperability, improved delivery of services and reduced cost of system operation and system sharing, where appropriate.

The Computer Security group oversees the protection of information processing resources to ensure that information and processing capabilities are reasonably protected from loss, misuse, unauthorized access, modification, unavailability, or undetected Activities. The goal of the group is to ensure that reliable data is available to the authorized user, when needed. The group is also responsible for all hardware with the means to store, manipulate, and deliver the data.

The IT Architecture team is a collection of Agency representatives with contractor facilitation. This team will be developing linked business, web and technology architectures, and a multi-year migration plan that support all aspect of the DOL.

10. Department of the Interior

The mission of the Department of the Interior (DOI) is to protect and provide access to the nation's natural and cultural heritage. The DOI ensures the U.S. honors trusted responsibilities to the Indian Tribes and upholds commitments to island communities. The DOI also protects the environment and preserves the country's natural and cultural resources. The department has four primary Assistant Secretaries: Policy, Management & Budget (PMB); Fish, Wildlife & Parks; Indian Affairs; Land & Minerals Management; and Water & Science. (See Figure 17.)

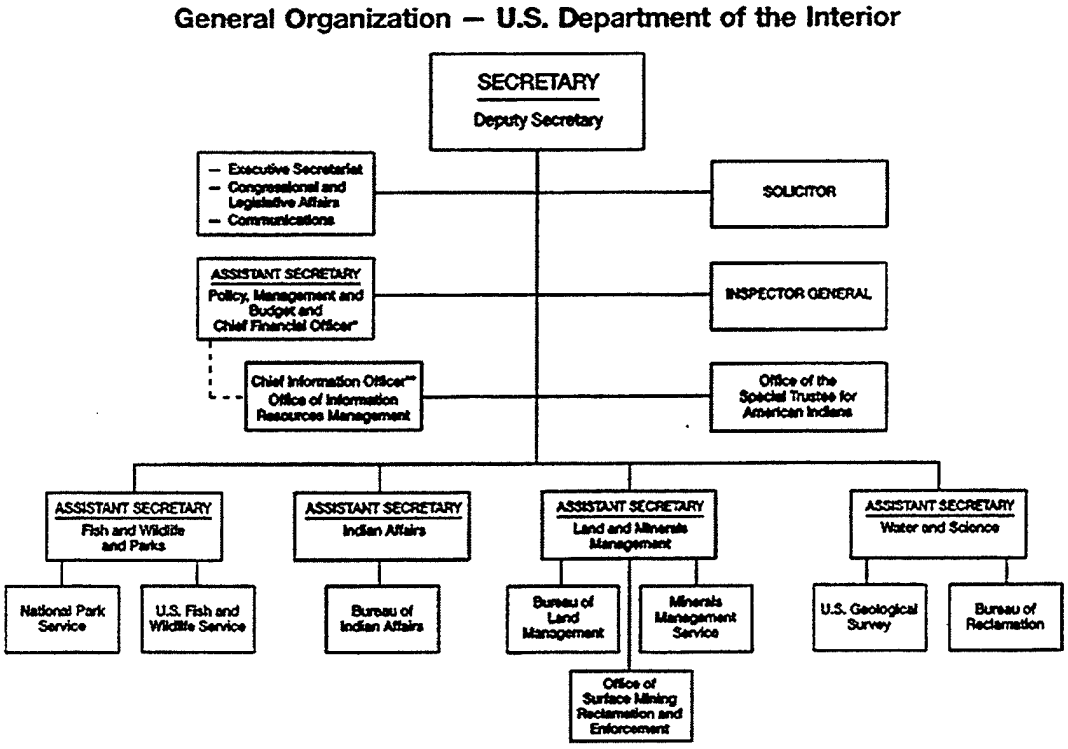

Figure 17. DOI Organizational Chart (as of Oct 2000) [From: doi.gov]

The DOI CIO heads the Office of Information Resources Management (OIRM). The CIO is responsible for continuously enhancing the ability of the Department to perform its many missions by efficiently managing information, providing sound technology investment solutions, and obtaining and improving access to information through the application of IT. The CIO ensures the alignment of IRM goals, objectives, and programs with the goals, objectives, and programs of the DOI and its' bureaus. The CIO is also responsible for optimizing the collection, access, and sharing of information/knowledge throughout the department using cutting edge IT.

The DOI CIO is responsible for numerous programs that fall within the realm of IRM. They include:

Records Management Program (RMP)	Government/Department Contracts	Privacy Program
Telecommunications Services Management Program	Radio Communications and Frequency Management Program	Information Technology Budget and Capital Planning
Department Webmaster's Council (DWC)	Department's Integrated Communications Network (DOINET)	Government Information Locator System (GILS)
Security Information Technology Security Program	Computer Training and Development	

Table 11. Programs of the DOI's CIO

11. Department of Education

The mission of the Department of Education (DOED) is to ensure equal access to education and to promote educational excellence for all Americans. A Deputy Secretary and an Under Secretary support the Secretary. The DOED structure consists of 8 program offices and 8 staff offices. [ed.gov]

The program offices include:

Office of Bilingual Education and Minority Languages Affairs	Office for Civil Rights	Office of Educational Research and Improvement
Office of Elementary and Secondary Education	Office of Postsecondary Education	Office of Special Educational and Rehabilitation Services
Office of Student Financial Assistance Programs	Office of Vocational and Adult Education	

Table 12. Program Offices of the DOED

The staff offices include:

Office of the Chief Financial Officer	Office of the Chief Information Officer	Office of the General Counsel
Office of Inspector General	Office of Intergovernmental and Inter-agency Affairs	Office of Legislation and Congressional Affairs
Office of Management	Office of Public Affairs	

Table 13. Staff Offices of the DOED

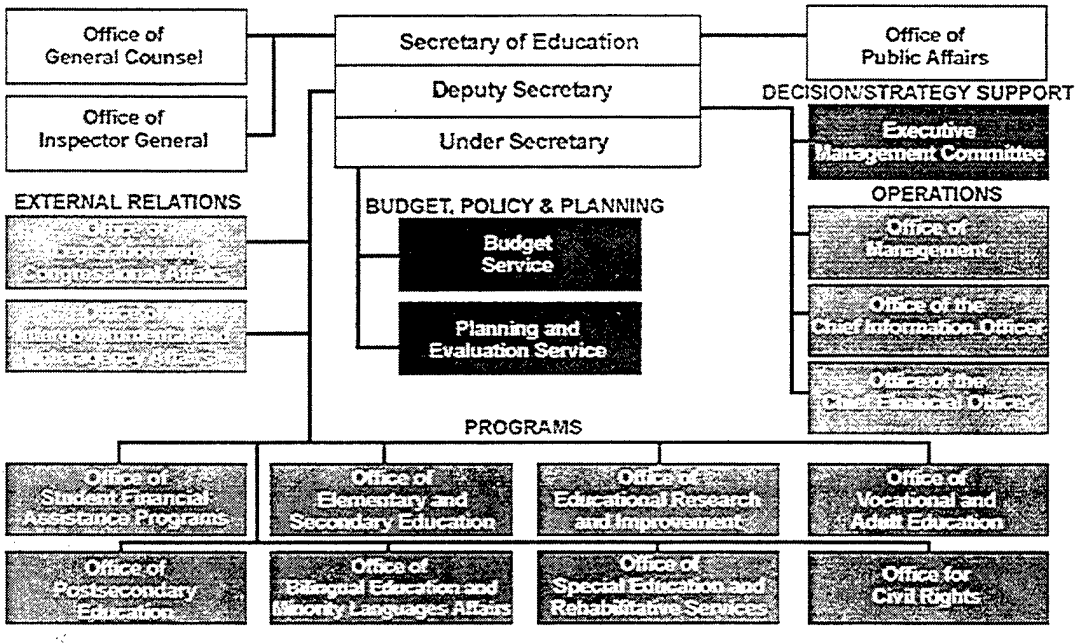

Figure 18. DOED Organizational Chart (as of Jan 2001) [From: ed.org]

The DOED CIO is an independent office that works for the Secretary of Education via the Deputy Secretary. The purpose of the Office of the Chief Information Officer (OCIO) is to provide world-class customer service to schools, students and their families through information technology. The DOED CIO is supported by three deputies in the areas of: Information Management (IM); Information Technology (IT); and Information Assurance (IA). (See Figure 19.)

The Deputy CIO of IM is responsible for planning, executing and evaluating all IM activities in the OCIO.

The Deputy CIO of IT provides technical support on all matters related to the department's network information systems. This deputy oversees the information systems architecture, network and telecommunications design and operations, configuration management and IT/IM contract management.

The Deputy CIO of IA is responsible for planning, developing, administering and evaluating all long and short-term IA activities in the department including the development and implementation of enterprise-wide IA and critical infrastructure protection programs.

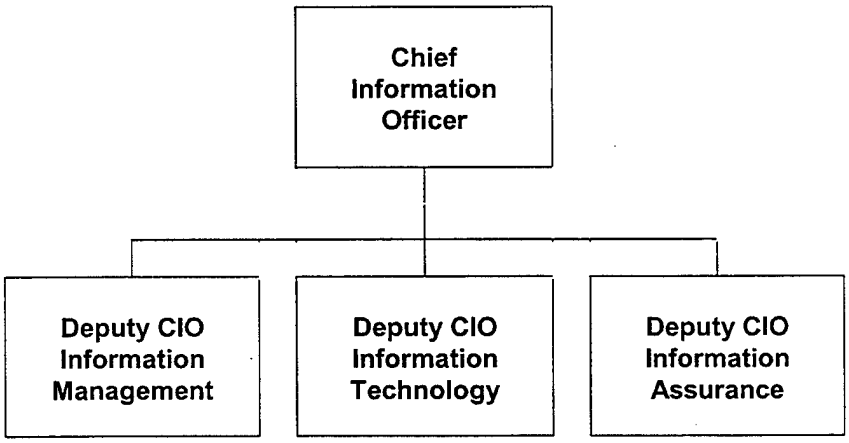

Figure 19. DOED CIO Organizational Chart (as of Dec 2000) [From: ed.gov]

12. Department of Veteran's Affairs

The Department of Veteran's Affairs (VA) administers laws the provide benefits and other services to veterans, their dependents, and their beneficiaries. The VA's mission is to serve as the principal advocate of Veterans, ensuring that they receive

medical care, benefits, social support, and lasting memorials. The VA is made up of several offices including: the Veteran's Health Administration (VHA); the Veteran's Benefits Administration (VBA); the National Cemetery Administration; the Board of Contract Appeals; Board of Veteran's Appeals; the Center for Minority Veterans; the Center for Women Veterans; the Office of Acquisition & Material Management; the Office of Alternate Dispute Resolution (ADR) and Mediation; the Office of Budget; the Office of Congressional Affairs; the Office of Employment Discrimination Complaint Adjudication; the Office of Financial Management; the Office of the General Counsel; the Office of Information & Technology (OI&T); the Office of the Inspector General; the Office of the Occupational Safety & Health; the Office of Planning & Analysis; the Office of Public Intergovernmental Affairs; and the Office of Small & Disadvantaged Business Utilization.

The Assistant Secretary for Information and Technology is the VA CIO. The VA CIO ensures that information and technology resources are maximized. The Office of Information and Technology is comprised of four organizational elements: the Office of Policy and Program Assistance, the Office of Telecommunications, the Austin Automation Center, and the Office of Information Technology and Administration. The VA CIO heads a council made up of the Deputy VA CIO, the VHA CIO, the VBA CIO, and representatives from the National Cemetery Administration, the Office of Planning and Analysis, the Office of Financial Management, and the Board of Veterans Appeals.

13. Department of Health and Human Services

The Department of Health and Human Services (HHS) is the principal agency for protecting the health of all Americans and providing essential human services. The HHS employs five Assistant Secretaries to include; Health, Management & Budget; Planning & Evaluation; Legislation; and Public Affairs. The HHS involves more than 300 programs spread over a wide spectrum. The several Operating Divisions (OPDIVs) divided up into two sections, Public Health Services and Human Services. (See Figure 20.)

Public health service operations include: the National Institutes of Health; the Food and Drug Administration (FDA); Centers for Disease Control and Prevention (CDC); Indian Health Service; Health Resources and Services Administration; Substance Abuse and Mental Health Services Administration; Agency for Healthcare Research and Quality.

Human service operations include: the Health Care Financing Administration; the Administration for Children and Families; and the Administration on Aging.

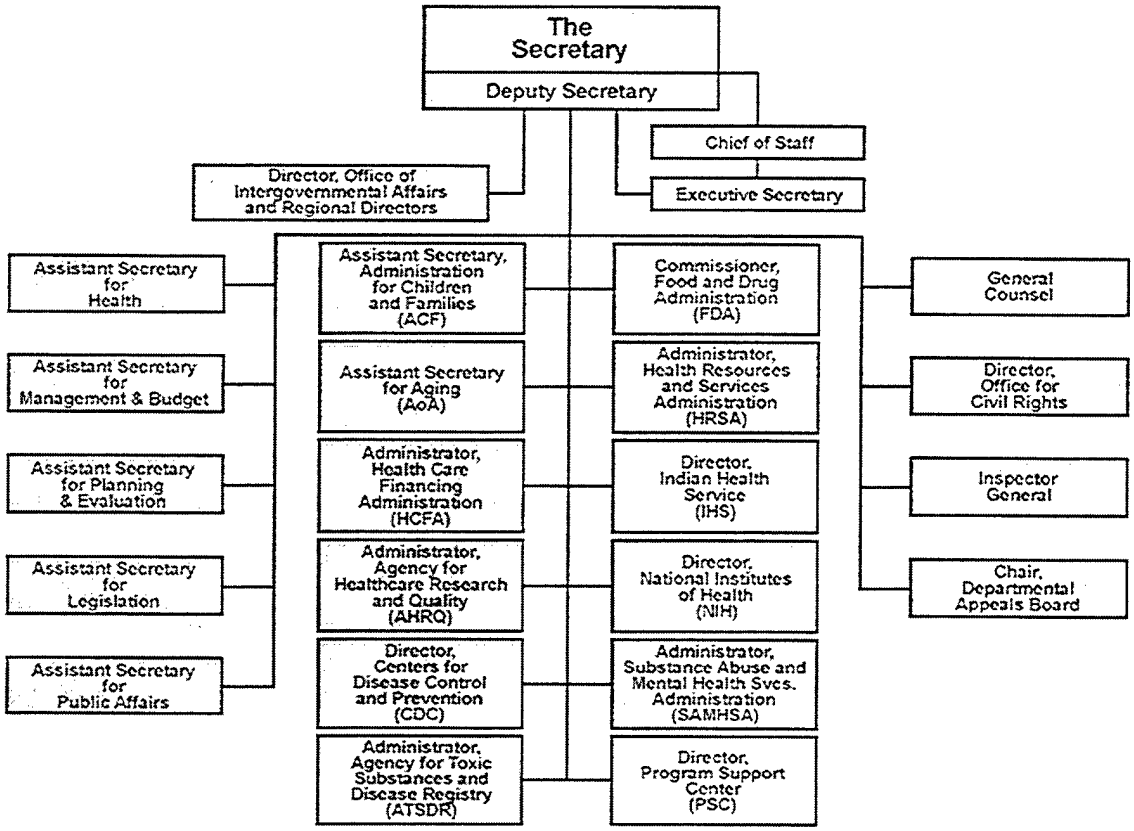

Figure 20. HHS Organizational Chart (as of Dec 2000) [From: hhs.gov]

The Assistant Secretary for Management and Budget (ASMB) is the HHS CIO and reports directly to the Secretary. The ASMB delegates authority for managing the IRM program to the Deputy Assistant Secretary for Information Resources Management (DASIRM), who also acts as the Deputy CIO.

The DASIRM provides leadership in the acquisition and use of computer technology and other information resources for the department. The DASIRM advises and supports the Secretary, the CIO and all of the OPDIVs concerning the planning and conduct IRM programs. The DASIRM provides IRM policy, guidance and strategic vision. In addition, the DASIRM oversees OPDIV projects and investments regarding IT.

14. Department of Housing and Urban Development

The mission of the Department of Housing And Urban Development (HUD) is to ensure that everyone has a decent, safe, and sanitary home surrounded by a suitable living environment. HUD creates opportunities for homeownership, provides housing assistance for low-income persons, and enforces the nation's fair housing laws and helps the homeless. HUD Headquarters (HQ) has two sides, program offices and support offices.

HQ Program Offices include:

Office of Housing	Office of Community Planning and Development	Office of Public and Indian Housing
Office of Fair Housing and Equal Opportunity	Ginnie Mae Foundation	Office of Multifamily Housing Assistance Restructuring

Table 14. HQ Program Offices of HUD

HQ Support Offices include:

Board of Contract Appeals	Chief Financial Officer (CFO)	Chief Information Officer (CIO)
Chief Procurement Officer (CPO)	Department Equal Employment Opportunity	Enforcement Center
Field Policy and Management	General Counsel	Labor Relations
Office of Administration	Office of Congressional and Intergovernmental Relations	Office of Healthy Homes and Lead Hazard Control
Office of Intergovernmental Relations	Office of International Affairs	Office of Small and Disadvantaged Business Utilization
Policy Development and Research	Real Estate Assessment Center	

Table 15. HQ Support Offices of HUD

HUD's CIO reports directly to the Secretary, and advises the Secretary and other HUD senior managers on the strategic use of IT in support core business processes and mission critical goals. The Office of the CIO is supported by: an Administrative Staff; the Office of Central Information Management; the Office of Systems Integration and Efficiency; the Office of Investment Strategies, Policy and Management; the Office of IT Reform and the Office of IT. (See Figure 21.)

The Administrative Staff advises and coordinates the internal management of resources available to the CIO.

The Office of Central Information Management is principal advisor to the CIO on the management of HUD's IT resources; IT Architecture; data administration; and information strategy planning.

The Office of Systems Integration and Efficiency is principal advisor to the CIO on configuration management, systems integration and design efficiency information systems. The office also manages the Business Process Improvement (BPI) Program and computer security.

The Office of Investment Strategies, Policy, and Management advises the CIO on IT policy/management and supports the Technology Investment Board Executive Committee (TIBEC). The office also oversees of the department's Reports Management Program that includes the Information Collection Budget.

The Office of IT Reform is responsible for all aspects of IT reform at the Department. This includes the IT investment strategy and capital planning program; the

TIBEC; IT capital planning and investment control; economic and risk analysis of proposed IT investments; and maintaining a information technology performance measurements program.

The Office of IT's mission is to deliver technical assistance, guidance, and support for national initiatives. The office also implements CIO policies, standards and guidelines.

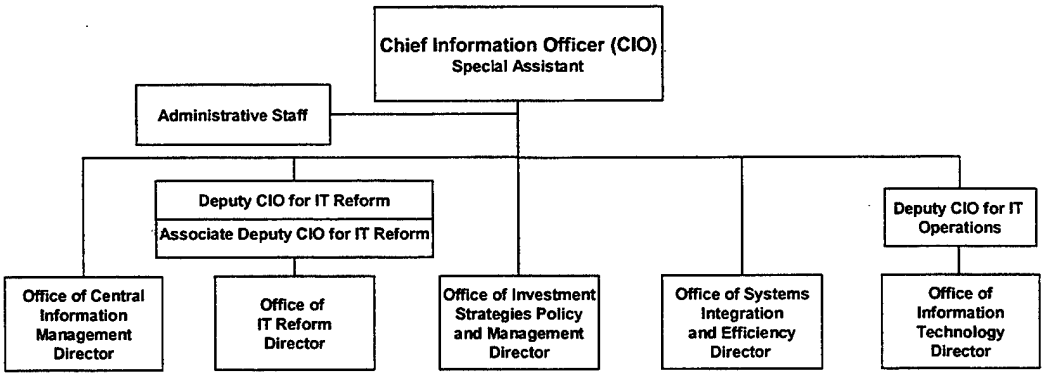

Figure 21. HUD CIO Organizational Chart (as of Oct 2000) [From: hud.gov]

15. Environmental Protection Agency

The mission of the Environmental Protection Agency (EPA) is to protect human health and to safeguard the natural environment including the air, water, and land. [epa.gov] The EPA is headed by an Administrator. The Administrator is supported by nine Assistant Administrator, three staff offices, and ten regional offices. (See Figure 22.)

The Administrators include: Resource Management; Air & Radiation; Enforcement & Compliance Assurance; International Activities; Environmental

Information; Prevention, Pesticides, and Toxic Substances; Research & Development; Solid Waste & Emergency Response; and Water.

The Offices are that of the Chief Financial Officer (CFO), General Counsel and Inspector General (IG).

Regional Offices are based in various cities around the country and represent a set area. Each EPA Regional Office is responsible for the execution of the Agency's programs, considering regional needs and the implementation of federal environmental laws. (i.e. the Seattle representative is responsible for the states of Washington, Oregon and Idaho)

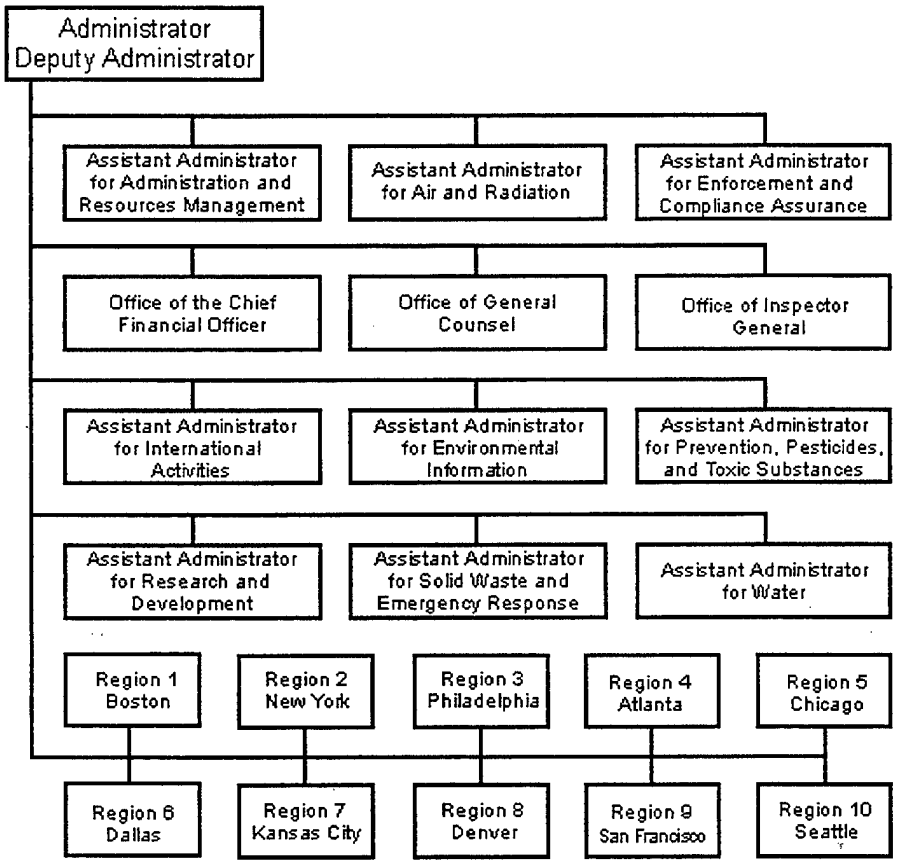

Figure 22. EPA Organizational Chart (as of Nov 2000) [From: epa.gov]

The Assistant Administrator for Environmental Information is the EPA's CIO. The Office of Environmental Information (OEI) has central responsibility over information management, policy and technology. The OEI supports the EPA's mission by integrating quality environmental information into the decision process. The OEI works with many different internal and external entities, to establish and oversee information-related policies and procedures.

The OEI is supported by five key groups: the Quality Staff; the Office of Information Collection (OIC); the Office of Technology, Operations and Planning

(OTOP); the Office of Information Analysis and Access (OIAA); and the Office of Planning Resources and Outreach. (See Figure 23.)

The Quality Staff develops agency-wide policy for QA, developing guidance and tools, providing training and outreach, and overseeing the implementation process.

The OIC develops and implements data collection policies and services. The OIC promotes efficient and effective collection/use of data.

The OTOP organizes strategic planning for IT and security. This office also sets hardware, software and telecommunications standards and operates the agency's internal technology infrastructure.

The OIAA develops policies for data analyses, data interpretation and the responsible use/release of data.

The Office of Planning, Resources and Outreach manages outreach and communication programs while ensuring the implementation of OEI policies, programs and procedures. The Office also assures sound strategic planning and resource management within OEI.

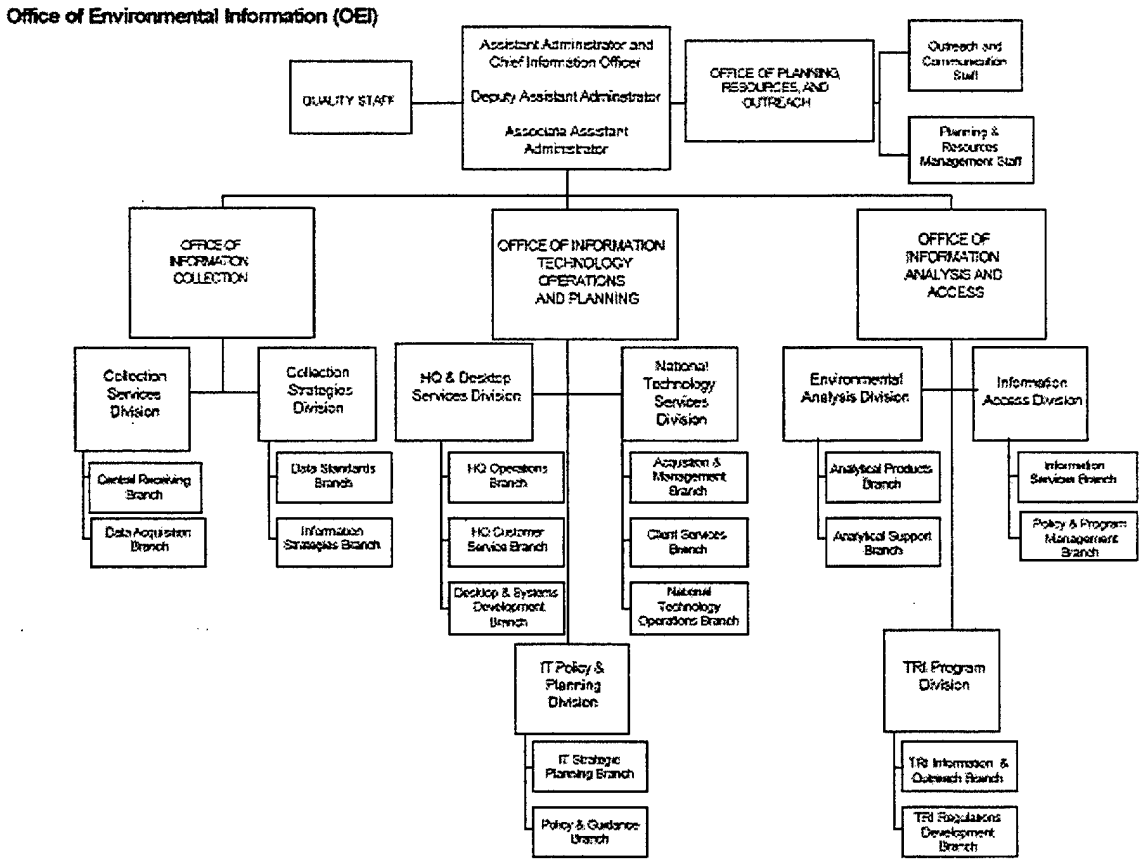

Figure 23. EPA OEI Organizational Chart (as of Dec 2000) [From: epa.gov]

16. Federal Emergency Management Agency

The Federal Emergency Management Agency (FEMA) is an independent agency of the federal government, reporting to the President. The purpose of FEMA is to reduce loss of life and property and protect critical infrastructure from all types of hazards via an emergency management program of mitigation, preparedness, response and recovery. [fema.gov]

FEMA's organizational structure mirrors the functions that take place in the cycle of emergency management: mitigation, preparedness, and response and recovery. FEMA

is supported by a robust structure to include nine support offices, five directorates, and ten regional offices. FEMA also contains the U.S. Fire Administration (USFA), which supports the nation's fire service, and the Federal Insurance Administration (FIA), which provides flood insurance nationwide. (See Figure 24.)

The nine support offices include: Inspector General (IG); Congressional & Legislative Affairs; Human Resources Management; Equal Rights; Public Affairs; Policy & Regional Operations; Financial Management; National Security Affairs; and General Counsel.

FEMA's directorates include: Mitigation; Recovery & Response; Information Technology Services; Preparedness; and Operations Support.

FEMA's ten regional offices are organized similarly to that of the EPA and they work directly with their states to help plan for disasters, develop mitigation programs, and meet needs when major disasters occur.

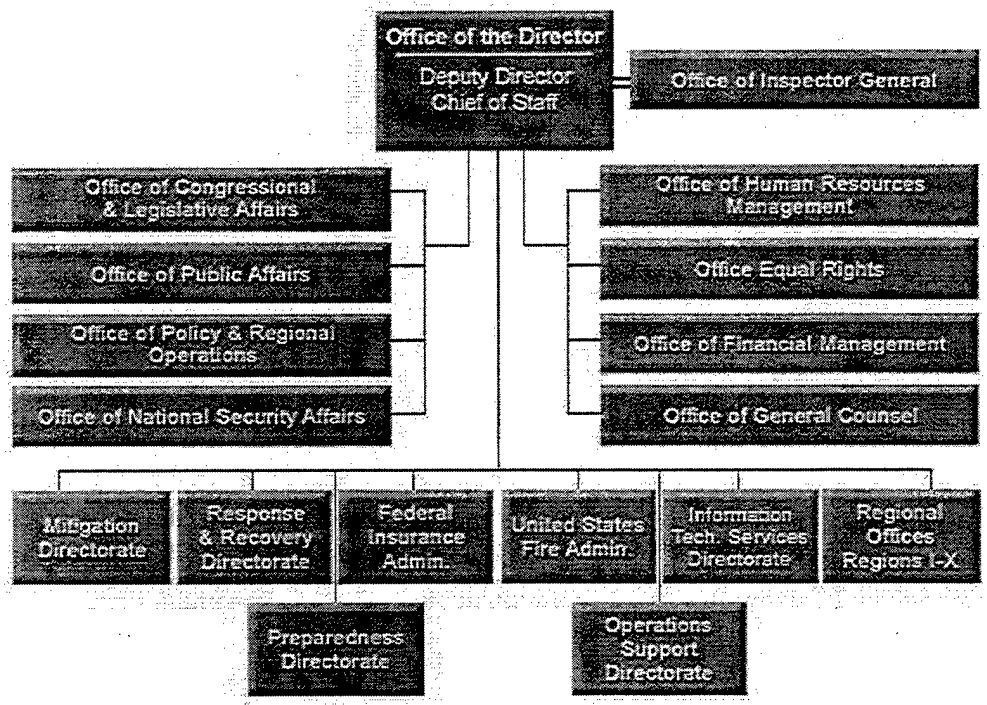

Figure 24. FEMA Organizational Chart (as of Dec 2000) [From: fema.gov]

The Information Technology Services Directorate provides agency-wide IT services and systems for routine operations and in emergency disaster situations. In concert with other federal agencies, state and local governments, this Directorate provides direction for integrating IT resources, automated data processing, communications, and information services necessary to expedite all aspects of the emergency management cycle.

The head of the directorate serves as FEMA's CIO and is responsible for IT policy & planning; agency-wide IM services and IT systems engineering. The directorate is supported by five programs including: IT Investments & Evaluations; IT Architecture; Management and Operations of Information Systems; FEMA Switched Network; and IT Security.

17. Central Intelligence Agency

The CIA is an independent agency accountable to the American people through the intelligence oversight committees of Congress. The CIA's mission is to support the President, the National Security Council (NSC), and all officials who make and execute U.S. national security policy. The CIA engages in research, development, and deployment of high-leverage technology for intelligence purposes. As a separate agency, CIA serves as an independent source of analysis on topics of concern and works closely with the other organizations in the Intelligence Community to ensure that the intelligence consumer receives the best intelligence possible.

The CIA is lead by the Director of Central Intelligence (DCI), who reports directly to the President. The DCI is supported by: the Deputy Director of Central Intelligence (DDCI); the Executive Director of the Central Intelligence Agency (EXDIR); the Deputy Director of Science & Technology; the Deputy Director of Operations; and the Deputy Director of Administration.

The DDCI assists the Director in his duties as head of the CIA and the Intelligence Community and exercises the powers of the Director when the Director's position is vacant or in the Director's absence or disability. The EXDIR manages the CIA on a day-to-day basis. The Director of Intelligence is responsible for the production and dissemination of all-source intelligence analysis on key foreign issues. The Director of Science and Technology creates and applies innovative technology in support of the intelligence collection mission. The Director of Operations is responsible for the

clandestine collection of foreign intelligence. The Directorate of Administration provides administrative support to the CIA in such areas as communications, security, human resources, and logistics. (See Figure 25.)

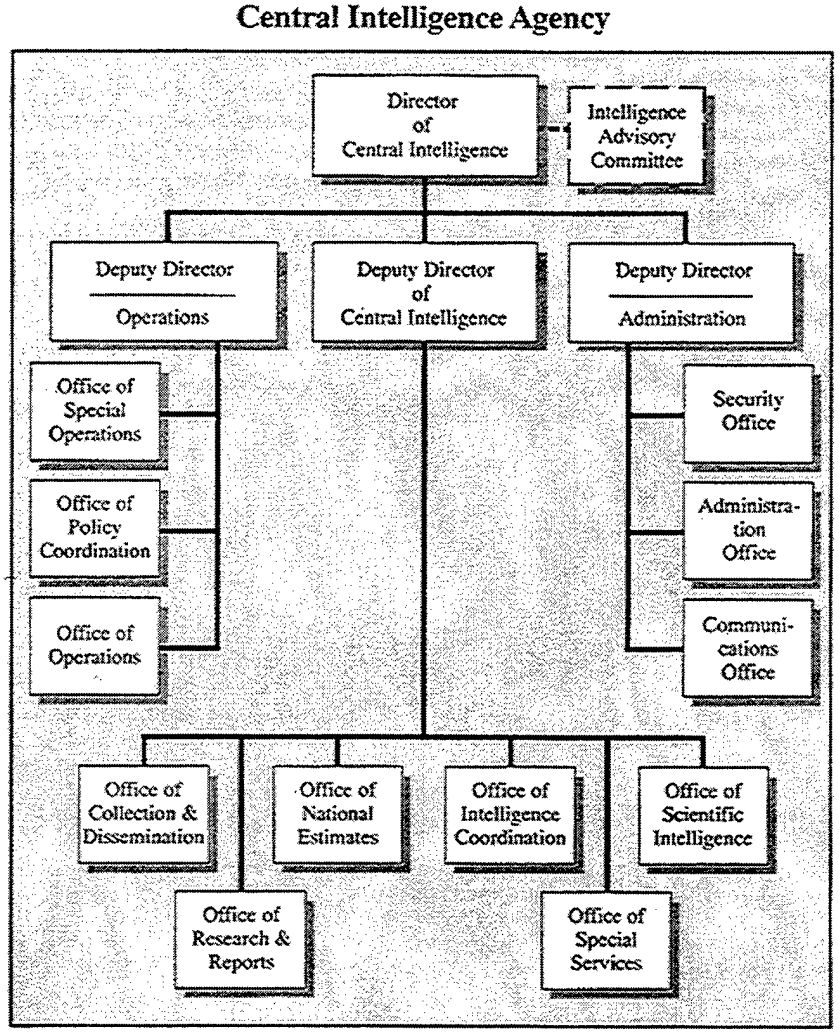

Figure 25. CIA Organizational Chart (as of Dec 1999) [From: cia.gov]

Within the CIA, there exists a conglomeration of government intelligence assets. This group is called the Intelligence Community (IC). At the top of the community is the National Intelligence Council (NIC). The community is comprised of National

Intelligence Officers, senior experts from both inside and outside government circles. The NIC concentrates on the substantive problems of particular geographic regions of the world and of particular functional areas such as economics and weapons proliferation.

The Intelligence Community Chief Information Officer (IC CIO), who is appointed by the DCI, is the agencies lead CIO. The IC CIO works with Community CIO's and other Information Systems (IS) leaders to shape enabling information systems and technology in response to the DCI's Strategic Intent. As a member of the IC, the IC CIO has direct contact with other intelligence agencies (Figure 26.) and as a result may better coordinate inter-agency IO concerns.

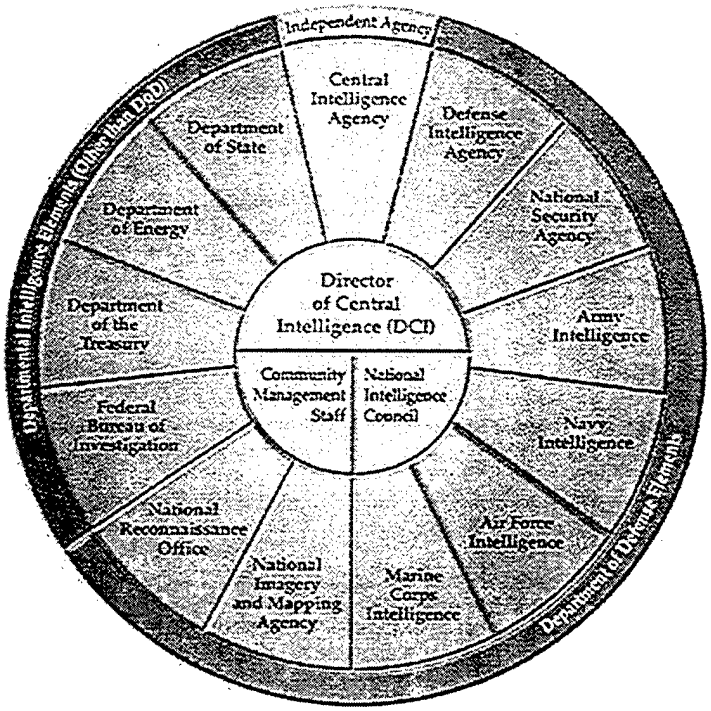

Figure 26. IC Members [From: odci.gov]

E. EVALUATIONS

Deficiencies of the current organization include: a lack of uniformity; a focus on the science side of IO; a lack of shared IO assets that results in redundancy; and a lack of incorporating intelligence assets.

1. Uniformity

Although each department must define and employ the services of their CIO to the best of their needs and abilities, they must have a uniform level of responsibility. It is the opinion of the authors that each CIO must be an independent entity within their organization that works directly for and with their respective Secretary/Director. The equality of responsibility would ensure that each CIO had a balanced influence on the council.

2. All Science, No Art

The current CIO Council is made up of what is conventionally thought of as "chief information officers." They maintain information services, structures and technologies. This is a purely technology-based view of Information Operation. The departmental/agency CIOs must be brought into the art side of the fold. This added responsibility demands a higher level of authority, and a greater range of capabilities. The purpose of the thesis is not to advise individual organizations (e.g. DOD, CIA, DOC) how to reorganize within, but to properly empower the CIOs. The authors believe that the

responsibilities of the CIO's must include both the science and the art aspects of IO. The bottom line is that each CIO must be responsible for all "information" in all mediums (i.e. intelligence assets, public affairs, civil affairs, information systems, and so forth.).

3. Redundant IO Assets

The lack of shared IO assets is a direct result of "All science, No Art". If CIOs were truly empowered to the degree that they were tied into everything from public affairs to intelligence assets, then they could effectively be able to share information. The sharing of information would result in common operating pictures, agencies would not have to deploy assets if another agency already had assets assigned. Information databases could be shared to whatever degree security would allow. How many DOJ assets, via the FBI, are committed abroad to counter terrorism and such, when quite possibly the CIA does much of the same? These are the kinds of questions individual organizations must ask and then explore through a common medium such as the CIO Council.

4. IO Intelligence

In continuing to integrate the "art" side into the scope of a CIO's responsibility, intelligence assets must be brought into the fold. The Intelligence Community (IC) looks like a microcosm of the CIO Council. Even though the two are currently unrelated, the IC has many of the same types of roles. Of course, the members of the IC only include those that pertain to national security (DOD, DOJ, DOS, CIA, etc.), but the authors believe that this community must be brought in to the realm of IO. This may be accomplished by

incorporating the IC in the form of a committee or a community within the CIO Council. In Chapter Six the authors discuss this very concept in terms of an Information Operations Security Council (IOSC).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RELATIONSHIP BETWEEN NATIONAL SECURITY, INFORMATION OPERATIONS, AND INNOVATION

A. PRINCIPLES OF NATIONAL SECURITY

1. Introduction

> For most of the last 300 years, states have dominated the international system. This domination may be coming to an end, driven in part because of the advanced information and communication technologies. These technologies will enable other types of international actors to challenge state dominance as never before. [Papp and Alberts, 1997, p. 700]

As the United States has entered the twenty first century, the global environment continues to be in flux. The fifty-year threat of global nuclear war with the Soviet Union is no longer present, but neither is the relative stability that accompanied that bipolar world. In fact, the world is certainly further away from this goal than it was before the fall of the Soviet Union. The Cold War has been over for nearly ten years and in that period the threats to national security have become diminished in potential, but increased in both number and uncertainty. The post-Cold War period has heightened the levels of uncertainty and in turn diminished confidence in United States national security. This is the global environment the United States will be facing in the foreseeable future.

The National Defense Panel identified four key trends that are main causes of the new global environment in a 1997 report, Transforming Defense: National Security in the 21st Century, to Secretary of Defense William Cohen. Theses four interrelated trends are listed below.

- The geopolitical revolution that prompted the collapse of the Soviet Union and that will see the emergence of China as a major regional and global actor.

- Demographic and social pressures of potentially volatile social systems.

- The emergence of a global, interdependent marketplace that affects the well-being of virtually every nation and society.

- The technological revolution that is transforming advanced industry-based economies into information-based economies and that promises to affect a revolution in military affairs.

These four trends have and will continue to have a profound affect on the global security environment, most notably in the information operations domain. It is certain that the future adversaries of the United States have learned from the Gulf War, in that they cannot confront the U.S. conventionally (Second Wave) with massed armies, or blue-water navies. The future adversary will try to find weaknesses or "chinks" in the armor and exploit them. They will focus on using weapons of mass destruction (WMD) against forward deployed U.S. military forces and quite possibly the continental United States. Additional threats could include terrorist actions (e.g. U.S. Embassies and USS COLE bombing) and information systems/infrastructure attacks (e.g. Denial of Service or computer virus).

2. National Interests

The national interests of the United States, although debated throughout history, have remained relatively constant. Many scholars have different interpretations of what

the national interests should be, but for the most part there have always been four constant themes. Donald Nuechterlein states in his book United States National Interests in a Changing World that "throughout the nation's history four long-term, enduring national interests have conditioned the way the U.S. government viewed the external world and this countries place in it." [Nuechterlein, 1973]

- Defense of the United States and its constitutional system.
- Enhancement of the nation's economic well-being and promotion of U.S. products abroad.
- Creation of a favorable world order (international security environment).
- Promotion abroad of U.S. democratic values and the free market system.

B. INFORMATION OPERATION'S ENVIRONMENT

1. Introduction

Information Operations are defined in Joint Publication 3-13 as "actions taken to affect adversary information and information systems while defending one's own information and information systems." This definition is specifically directed towards information operations in the military, but is also applicable in regards to overall IO and national security. One must take the view that information operations is not strictly a military concept, but a global concept that is also quite prevalent in the commercial business and government sectors. Only then, with this view of a global IO concept, can the depth of information operations be explored, realized and utilized.

The importance of Information Operations in terms of protecting vital national interests cannot be overstated. The United States must maintain its lead in information systems and technology. The fact that commercial progress and growth in information technology is so extensive, coupled with the fact that these technologies are relatively cheap and easily accessible, will present adversaries with opportunities that they have not had in the past. Also, the more reliance the United States puts on these information systems and technologies economically, commercially, and militarily, the more vulnerable the nation will be to such an attack.

The global information environment expands exponentially almost every day. The combination of different IO elements (e.g. industry, global politics, information infrastructure) constantly changes the operating environment. Figure 27 illustrates the various factors involved in shaping the global Information Operations environment.

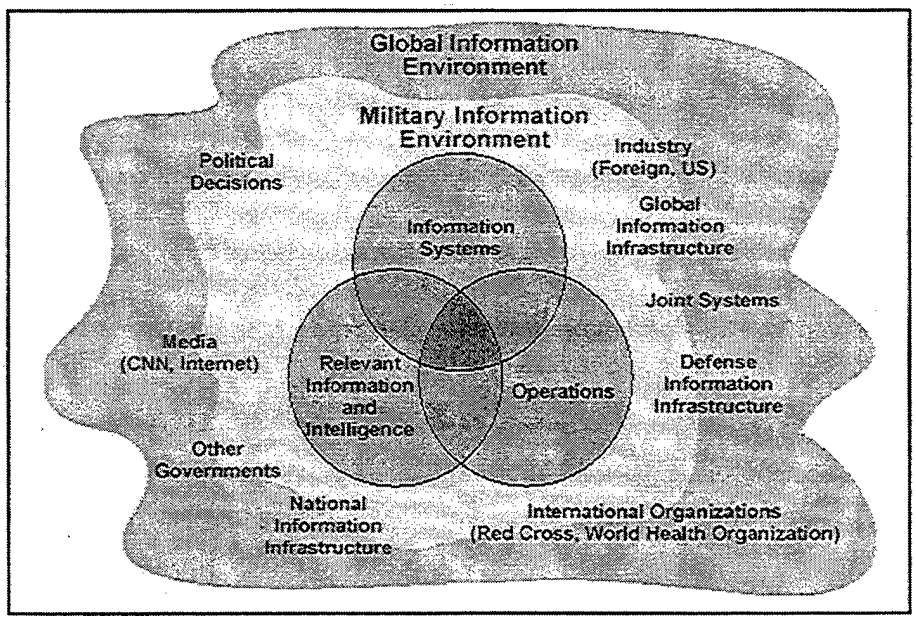

Figure 27. Global Information Operations Environment [From: HQ USA FM 100-6, 1996]

2. Activities in the Information Operations Environment

There are several critical actions that can be taken by an individual or organization in the IO environment, as depicted in Figure 28. These actions can be taken simultaneously or in some type of chronological order, dependent upon the situation and goals of the individual or organization. They are not always mutually exclusive or strictly dependent upon each other. It will be helpful to briefly discuss each of these actions and their effects on the IO environment.

a. Acquire

Information can be acquired through a variety of ways, including but not limited to: intelligence, personal experience and expertise, technical surveillance, and inter-organizational relations and communications. Acquiring information has become

one of the easier tasks in the Information Operations environment. The difficulty that many face is in acquiring information that is relevant to the goals of the individual or organization and receiving the information at the right time. In many cases, organizations take the approach that "more is better" and accumulate masses of useless information (information overload) or spend so much time collecting information that they lose the opportunity to use it to their advantage.

b. Protect

The protection of information is quickly becoming one of the focal points of all organizations (including commercial, government, and military). Information protection must be kept at three levels: human, physical, and technological/electronic. The human level is basically comprised of effective Information Assurance and Operational Security. The physical level is the corporal security of the organization's information centers and headquarters and its protection from intruders. The electronic level, similar to the physical, is designed to prevent intruders from accessing information in the electronic information center or databases. This type of security is certainly the most difficult to maintain in today's environment.

Organizations are finding it harder and harder to protect internal information from their adversaries. Part of the reason for this problem is because of the fact that commercial progress and growth in information technology has been so extensive during this Information Revolution. A second contributing factor is that these technologies are relatively cheap and easily accessible which allows adversaries with

opportunities that they have not had in the past. Protection of information will continue to be one of the most difficult aspects of the IO environment

c. Exploit

Exploitation is basically the use or manipulation of an adversary's data without their knowledge. Exploitation could be as simple as monitoring an adversary's information system or, on a more complex level, corrupting crucial data or databases. Exploitation of information is abundant in corporate and state espionage and even more so in the military where international laws become ambiguous.

d. Deny

Denial of information goes hand-in-hand with information exploitation. Once an adversaries information has been exploited, it opens the door for some types of information denial. Denying an adversary critical information degrades the overall efficiency and effectiveness of the system and forces the adversary to rely on other means of information for decision-making. A classical example of the exploitation-denial relationship is a Distributed Denial of Service for a computer server. This is where the attacker "cases" a network via traffic flow analysis to identify vulnerable nodes and then floods those nodes with an onslaught of pings and requests, thus relegating the network unusable.

e. Use

The use of information is synonymous with organizational decision-making. Once the information has been acquired, analyzed, disseminated and fully

understood it can then be utilized in making a decision for a particular situation or used in a future planning process. This process, known as the cognitive hierarchy, which will be further discussed in Chapter Five.

f. Manage

Management of information is the basis of an effective command, coordination, and control system. It entails getting the right information, in the right format, to the right people, at the right time. The keys to accomplishing these tasks are having a well-connected system that is resilient and maximizes information throughput. An effective information management system will promote information flow both horizontally and vertically within an organization. Information and knowledge management will be discussed in greater detail in Chapter Five.

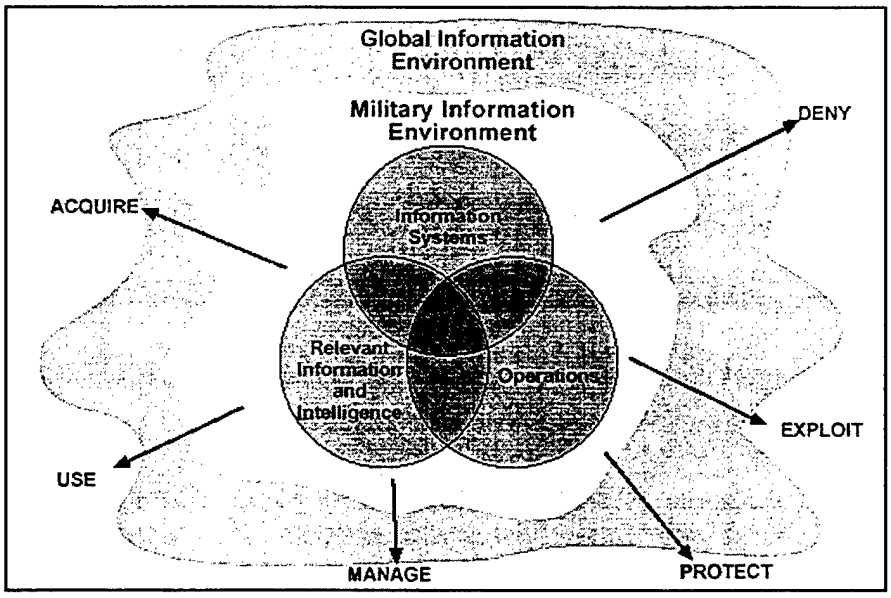

Figure 28. Information Operations Activities [From: HQ USA FM 100-6, 1996]

C. INFORMATION OPERATIONS AND THREATS TO NATIONAL SECURITY

1. Introduction

The 1999 report, from the Executive Office of the President, A National Security Strategy for a New Century identifies six principle threats to the national security of the United States. These threats are:

a. Regional or State-Centered Threats

Numerous states have the capability to threaten the United States through aggression. These threats have increased their offensive capability and in most cases possess, or have access to WMD. These states include, but are not limited to Iraq, Iran, China, and North Korea.

b. Transnational Threats

Threats that have no boundaries or borders and can threaten both United States interests at home and abroad. These actors are most likely to be rogue states, terrorist organizations, or criminal syndicates. This threat is especially important in the IO environment because it involves the critical infrastructures of the United States. Cyber-attacks will be the weapons of choice in addition to traditional physical attacks and sabotage.

c. Failed States

This threat is a direct product of the post-Cold War global instability. Many states are unable to provide the basic governance, safety, security and opportunities for their people and in turn are prime candidates for insurrection and instability. The result is often civil unrest, war, migration or mass famine. These states often request some type of assistance or aid (e.g. humanitarian). In some instances, the United States is compelled to intervene because the regional instability directly affects national interests.

d. Spread of Dangerous Technologies

The proliferation of weapons of mass destruction (WMD) is the central factor associated with this threat. Rogue states and terrorist organizations pose the largest concern when it comes to this threat. Rogue states, knowing they cannot contend with the United States in conventional military actions will resort to the threat and possible use of WMD. Terrorist actions could also quite possibly shift from conventional bombings and hijackings to the use of WMD. A second type of technology that is not addressed by the previously mentioned report is Information Technology. Certain information technologies that have the capability to shut down or seriously degrade the nation's critical infrastructures can have just as damaging an effect as WMD.

e. Foreign Intelligence Collection

With the infusion of information technology into the global environment the capability of foreign intelligence agencies has increased tenfold. The fact that the United States is so dependent on networks and information systems is actually a detriment to national security. The nature of the global information infrastructure leaves many information systems vulnerable to anonymous penetration and attack. This gives both traditional and unknown adversaries the ability to collect intelligence on United States military and government policies and operations.

f. Environment and Health Threats

This threat is often overlooked, but it has serious ramifications to the national security of the United States. History shows that epidemics (e.g. polio, tuberculosis, AIDS) have almost annihilated populations. Adversaries could quite conceivably introduce a life-threatening disease into the United States without any detection. For instance, what would be the ramifications if an adversary introduced a strain of the recent "Mad Cow Disease" from Europe into the United States cattle population? The results would catastrophic.

Each of these six threats, have a direct relationship with Information Operations. The confronting of these threats will become even more dependent upon effective Information Operations in the future global security environment. One must take the point of view that the correlation between the previously mentioned threats and

information operations lays at the intersection of technology and "soft" perception techniques.

D. DOCTRINAL AND ORGANIZATIONAL INNOVATION

1. Introduction

Webster's dictionary defines innovation as " 1. something new or different, such as a change in customs or ways of doing things; 2. an introducing or bringing in something new."

Contrary to common belief, innovation is not necessarily only related to technological advances and inventions. In fact, technological advances are more often than not the precursors to innovation. True innovation should be viewed as the culmination of changes in organizational thinking and strategy, doctrine, and technology. Barry Posen states in his book, The Sources of Military Doctrine, "The benefits of innovation can be judged, in part, in terms of its effect on integration. Do the means and ends retain a working relationship to each other? In part, innovation must be judged in terms of the general [organization] and technological environment." [Posen, 1984, p.29]

Effective innovation requires visionary thinkers who look beyond the scope of the present situation and environment. These individuals are often more than willing to voice their views will little regard to the "status quos." History has shown that these "out of the box" thinkers are often dismissed because their ideas/visions seem impossible to facilitate to the traditional old school thinkers. One visionary that comes to mind is Sir

Hugh Dowding, Commander of Great Britain's RAF Fighter Command and his endeavors in the Battle of Great Britain during World War II. The successful defense of Great Britain was a direct result of Fighter Command's highly effective and efficient information and intelligence systems, as previously discussed in Chapter Two. The effective use of these systems was a direct result of Sir Dowding's doctrinal and strategic innovations within Fighter Command. A second, modern day innovator/visionary is Vice Admiral Arthur Cebrowski, founder of U.S. Navy's Network Centric Warfare. VADM Cebrowski continues his efforts to innovate in the Unites Sates Navy through the incorporation technology, doctrine and the global environment.

Organizational innovation is just as important as technical or doctrinal innovation. Changes and advancement in technology and doctrine quite often require than some type of organizational innovation, or at least an organizational review take place. These organizational changes are starting to take place at the governmental levels, but unfortunately, they are being met with a substantial amount of resistance from those who are comfortable with the "old school" (or Second Wave) thinking that what worked yesterday will work tomorrow. The Executive Office of the President stated the need for organizational innovation within the U.S. government in 1998 via A National Security Strategy for a New Century:

> We must continue aggressive efforts to construct appropriate twenty-first century national security programs and structures. The Defense Department, State Department and other international affairs agencies are similarly reorganizing to confront the pressing challenges of tomorrow as well as those we face today. Federal, state, and local law enforcement and emergency response agencies are enhancing their ability to deal with terrorist threats. Government and industry are exploring ways to protect

> critical national infrastructures. We will continue looking across our government to see if during this time of transition we are adequately preparing to meet the national security challenges of the next century. [The White House, 1998]

E. CONCLUSION

Thomas Friedman says it best when it comes to the lack of innovation and unwillingness to change in his book The Lexus and the Olive Tree. In comparing the Cold War system to the present system of globalism he states that adaptation and change have been slow to take place because the "old system" is what individuals know and are comfortable with. In the Cold War system they adversary was known, the environment was defined, and the strategy to deal with the adversary in this environment was planned out. The system of the past ten years, globalization, is much more complex. The threats are much more ambiguous and the traditional boundaries are no longer there. Friedman explains some of the possible reasons for this resistance to change in the following excerpt from his book.

> The foreign policy community has been slow to adjust to this system for a variety of reasons. In part because it is still too new and our experience with it still too limited. In part it is because people who are life-long experts in one thing – the Cold War- don't want to be told that their expertise is not going to take them very far in analyzing geopolitics in this new system, and so they try to dismiss it. In part it may be due to the rather unheroic nature of many of the foreign policy issues that arise in this system.... Finally, the adjustment in seeing today's system has been slow in part because there is a certain allergy within parts of the foreign policy establishment to bringing markets and finance into the analysis. It is like talking about money and markets is unseemly or unmanly when analyzing geopolitics. [Friedman, 1999, p.211]

Steps must be taken within the government, in both structure and thinking, to ensure that when matters of National Security and interests are discussed, Information Operations are synonymous with those discussions. These steps will only occur if individuals are able to accept the changes in a dynamic global environment and then be willing to adapt innovative measures. IO cannot be considered a separate issue. IO must have a place in all matters of national security.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ORGANIZATIONAL SCIENCE METHODOLOGY

A. INTRODUCTION

The basic definition of any organization is that it is " a consciously coordinated social entity, with a relatively identifiable boundary, which functions on a relatively continuously basis to achieve a common goal or a set of goals." [Robbins, 1990, p.4] Organizations vary in structure, size, environment, and purpose, but the underlying fact that makes all organizations similar is that they are together to achieve a relatively common goal or end state. Of course the individuals within any organization will have their own personal motivations and goals, but the culmination of the achievement of those personal goals will inevitably lead to overall organizational prosperity. Charles Perrow accurately describes the issue of organizational goals in his book Complex Organizations: A Critical Essay. Perrow states "....goals are set by the leaders and then broken down into sub goals at each level of the organization. Each lower-order goal becomes a means to a high-order goal. People do not accept these goals because they necessarily share them or believe in them, but because the organization has mechanisms to insure that working toward them meets the individuals own personal values." [Perrow, 1972, p.150] Therefore, organizational success is fairly dependent upon the success of the individuals within that organization.

1. Organizational Design

An organizational design has often been perceived simply as the structure of an organization, but it is more accurate to define an organizational design as a system that includes the organization's structural alignment, management processes, information systems, reward systems, and people within the prescribed strategy. [Galbraith, 1987]

Organizational design is focused on how an organization should be structured according to its goals. Organizational structure is basically the "nuts and bolts" of the organization; it directs how tasks are allocated, who is responsible for the completion of those tasks, and how the formal coordination between individuals actually takes place. Organizational design looks at an organization's structure and tries to determine how constructing, altering, and innovating the organization's structure can improve overall operations to fulfill the preset goals more efficiently and effectively. Design "is concerned with how things ought to be, with devising structures to attain goals." [Simon, 1981, p.133] Its prescribed goals and missions determine an organization's boundaries and how they relate to the environment. There must be a direct and definitive relationship between an organization's design, environment, and goals; if there isn't then the organization will incur some type of misfit. This relationship (See Figure 29.) will therefore play an integral part in the overall development of the organization's strategy and design.

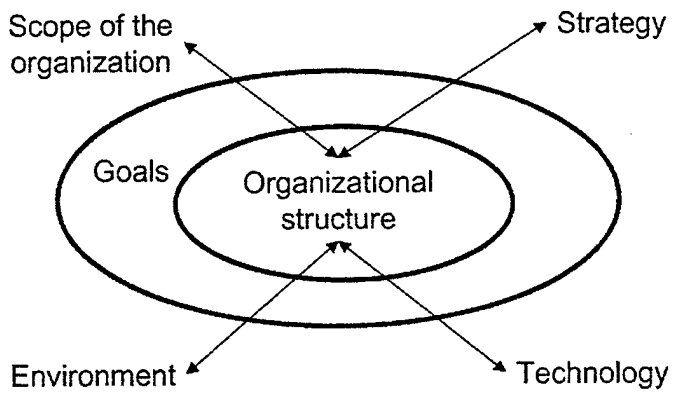

Figure 29. Organizational Design [From: Erickson, 2000]

2. Efficiency, Effectiveness and Viability

There are three fundamental criteria that are required for any organization to be successful. They are independent of size, environment or purpose. These three criteria are effectiveness, efficiency, and viability. Effectiveness, meaning that the organization's purpose is realized and the goal is accomplished. Efficiency, meaning that the organization uses the least amount of resources to achieve the goal. And lastly, viability, meaning that the organization can withstand changes in the environment and persevere for a long period of time. [Burton and Obel, 1998, p.4]

In some instances efficiency and effectiveness contradict one another. Organizations can be highly effective and at the same time be extremely inefficient or an organization can be exceptionally efficient while not accomplishing any of the goals that it has set forth. For example an organization may use every available resource at its

disposal to achieve its goals, but if the operations were planned better the organization may have come to the realization that the use of all their resources was not required. This is the case of an effective-inefficient organization. The efficiency versus effectiveness argument has always been somewhat of a "give and take" relationship with organizational structure. The ideal organization would of course be both efficient and effective.

Coordination among the separate groups or individuals within an organization is essential for the overall organizational success. "The fundamental issues in designing an organization are to group the small activities together so that the goals are realized or conversely, is to take a large task and break it into smaller tasks." [Burton and Obel, 1998, p.3] In either case the smaller tasks will eventually be brought together in order to fulfill the larger organizational goals. This process requires meticulous coordination, because without coordinating the smaller tasks and groups all the organization is left with is a collection of separate activities. In order for any organization to effectively coordinate they must utilize some type of information/communication system. To best accomplish this goal of effective coordination, the organization should to integrate the concepts of information processing and knowledge management at all levels. These concepts will be further analyzed in this chapter.

B. STRUCTURAL DETERMINANTS

An organization's structure is determined by countless factors. Some of these factors include, but are not limited to, size, operating environment, product/service provided, and overall competitiveness. In an analysis of an organization's structure the

organization's horizontal and vertical differentiation, its command and control, and the centralization/decentralization of decision making within the organization must be examined. Also essential is how the organization will "fit" with its external environment and overall goals.

A common organizational theory is the "rational system." In this system "theorists emphasize organizational goals, roles, and technology, and they look for ways to develop structures that best fit organizational purposes and environmental demands." [Bolman and Deal, 1991, p.9] A second theory is the "human resource" theory. This theory focuses on the relationship between the individual's needs and skills and their prescribed function within the organization. A third theory is the "political theorists," which is focused on the managerial understanding and use of power to achieve organizational success. [Bolman and Deal, 1991, p.9] Each of these theories offers a different point-of-view on how an organization should be structured in order to achieve success, but in actuality there is no "right" theory or structural system. A successful organization will have attributes of many different theories dependent upon the existing environment and organizational mission.

In essence, an organization must find the most effective and efficient combination of strategy, structure, individuals, rewards, processes, and the environment in order to achieve its goals in a given environment. All of these factors are interrelated and hold a strong bearing on one another. If there were a change in one of these factors it would inevitably require some type of change or adjustment in the others. Figure 30 displays how the concepts are interrelated.

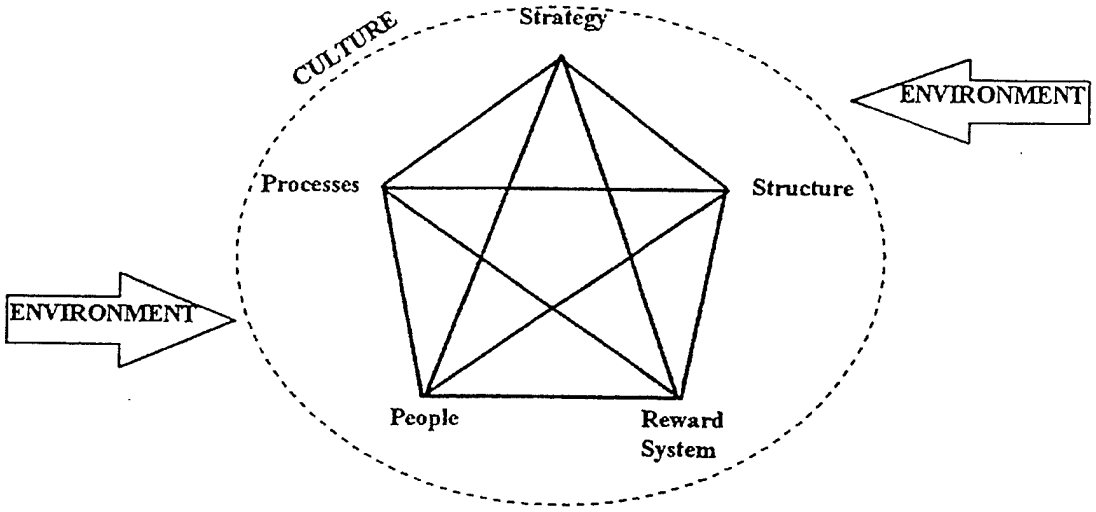

Figure 30. Star Model [From: Berger, 1998]

C. INFORMATION PROCESSING AND TECHNOLOGY

1. Introduction

Information in its' simplest form is defined as data that is collected from the environment and processed into a usable form. Any given piece of data is basically useless in its raw form. Only when it is processed does gain some type of use and meaning.

Information management is the cycle of processes that support an organization's activities and operations, it identifies and stores that information, and eventually develops and uses that information to achieves its goals. Information is not only needed about specific instances, but also for the development of new theories and frameworks that may

dispute currents organizational beliefs and standards. Information processing is used by organization to coordinate the different activities among its groups or individuals. "By processing information it (the organization) observes what is happening, analyzes and makes choices about what to do, and communicates the above to its members." [Burton and Obel, 1998, p.4]

Information is recognized as a strategic resource that must be effectively managed in order to maintain a competitive advantage in an organization's ever-changing environment. It plays a critical role in reducing uncertainty, and structural complexity. It also provides greater situational awareness for the entire organization.

2. Technology

Technology plays a key role not only in information processing, but also in the overall evolution of an organization's structure and design. Routineness of technology can often determine the level of complexity; this is illustrated in Figure 31, and centralization within an organization. Often routine technology is associated with organizations of low complexity. The reasoning for this association is that the more routine the technology is the less training is required for the individuals who use that technology. The same tends to hold true holds for an organizations level of centralization.

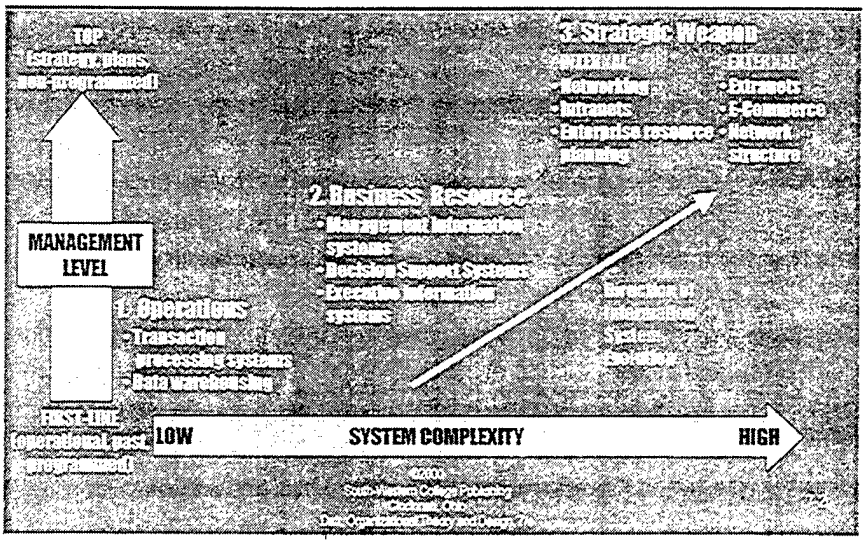

Figure 31. Evolution of Organizational Applications of Information Technology [From: Nixon, 2000]

The introduction of new technology will more often than not stimulate some amount of organizational learning. New technologies (e.g. information processing, telecommunication, decision support systems) open the door to new ways of accomplishing tasks, allow organizations to modify or even dismiss the previous procedures, and often require organizational reconfiguration to some degree. If done correctly the organization capitalizes on the benefits of the new technology and in turn often increases organizational effectiveness.

Gareth Morgan states that the organizations that do not incorporate these new and revolutionary changes in technologies into their organizational structures will eventually suffer severe consequences. Morgan view on this situation is stated below.

> Information Technology - in the form of micro computing, electronic communication, and robotics – has the capacity to transform the nature and structure of many organizations and the nature and lifestyles of their products and services. Organizations that fail to get "on board" and to

> reap the potential benefits will find the competition passing them by. The technology is leading us into a new age in which completely new styles of organization and new managerial competencies will come into their own. [Morgan, 1988, p.9]

3. Information Processing

There are some who believe that the problem of organizational design is actually an information-processing problem. Galbraith writes "the greater the uncertainty of the task, the greater the amount of information that has to be processed between decision-makers." [Galbraith, 1974, p.28] If information processing creates uncertainties in task performance then the information processing is referred or passed up the organization's chain of command (hierarchy) so that it can be reviewed. If an organization ignores the problems that are created from uncertainty, then organizational performance will be reduced. The downside to this hierarchal process is that the uncertainties often exceed the capacities of the decision makers. This, in turn, produces the unwanted scenario of "information overflow" and impairs the organizational performance. Organizations can either reduce their need for information processing or increase their capacity to process the information. [Galbraith, 1974, p.30] The disadvantage to reducing the need for information processing is the organization, to some degree, will lack the proper coordination and possibly incur high opportunity costs. Increasing the organization's processing capabilities is often the better alternative, but this will require an increase in resources. "In a hierarchical organization, the hierarchical processing of information can be increased in an investment in a vertical information system. The demand for

information processing capacity that arises from uncertainty frees the organization to be able to react to unforeseen events." [Burton and Obel, 1998, p.6] Although the demand for information processing and capacity continues to grow within organizations, the relative cost of processing that information has decreased, thus making increasing information capacity a viable option for many organizations. Lastly, according to Galbraith, "the task information requirements and the capacity of the organization to process information are always matched. If the organization does not consciously match them, reduced performance through budget overruns, schedule overruns, act. will occur in order to bring about equality." [Galbraith, 1977, p.55]

Figure 32 illustrates the "data to understanding" hierarchy within a given organization. The raw data that is collected is analyzed and filtered to produce pertinent information for the organization. This information is then further processed and distributed throughout the organization to generate a general knowledge base by means of cognition. This knowledge base is then transformed, through individual judgment, into understanding. Once this understanding is achieved by the organization's decision-makers the decisions can be made that support the organizational goals and mission. Although understanding gives decision-makers the ability to act, it does not necessarily mean they must take action. This knowledge must be further managed and constantly updated.

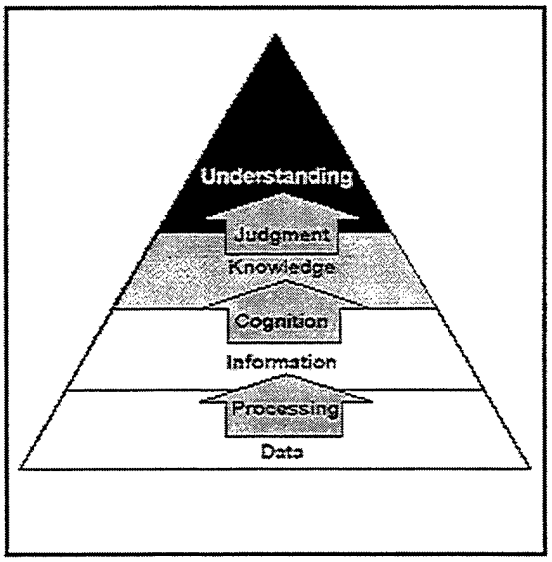

Figure 32. Cognitive Hierarchy [From: HQ USA FM 100-6, 1996]

D. KNOWLEDGE MANAGEMENT

> More than other structures, the power derived from the knowledge structure comes less from coercive power and more from consent, authority being conferred voluntarily on the basis of shared belief systems and the acknowledgment of the importance to the individual and to society of the particular form taken by the knowledge--and therefore of the importance of the person having the knowledge and access or control over the means by which it is stored and communicated. [Strange, 1988, p.118]

1. Introduction

Knowledge is basically information that has been tested and is accepted by an individual or organization. Knowledge is validated either through human cognition (Figure 32), or through some type situational analysis.

Knowledge management is centered on getting the right information to the right individual or group, in the right form, at the right time for the right purpose. Information provides the "what is happening" aspect to the organization, but that is not enough. The

organization needs to know "if" and "how" that information is relevant, and "who" needs the information, this is the knowledge management process. Knowledge management involves the identification and analysis of the information that could be pertinent to one individual in an organization and useless to another, or it may only be pertinent if coupled with other information. It is dependent upon the view of a single individual. Knowledge management involves the identification and analysis of available and required knowledge assets and knowledge asset related processes. These processes include developing the knowledge; preserving the knowledge; using the knowledge; and sharing that knowledge throughout the organization.

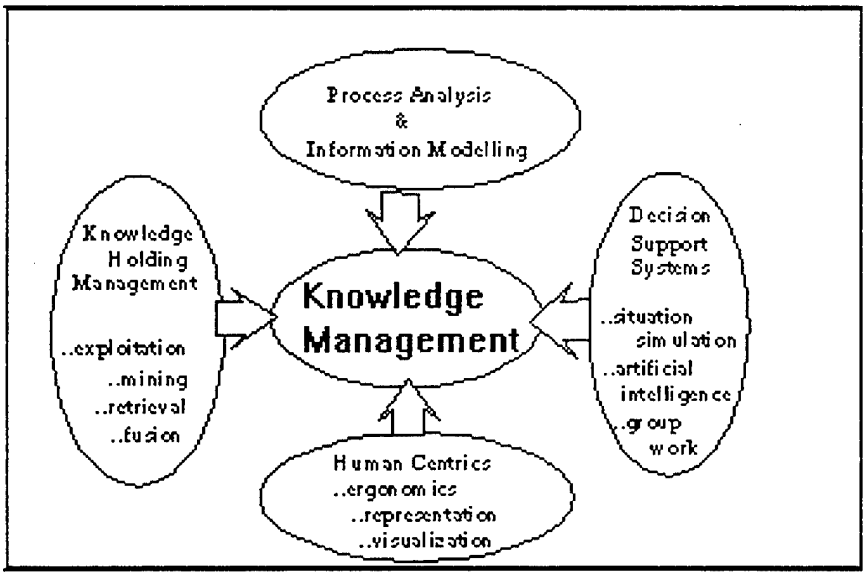

Figure 33. Knowledge Management Supporting Technologies [From: Garigue, 1995]

2. Knowledge Management Framework

The knowledge management framework is a step-by-step process that determines the most efficient and beneficial use of information/knowledge within an organization. There are four fundamental steps to the process and within each step there are operational questions about the knowledge that should be addressed. The basic framework is depicted below. [Van Der Spek and De Hoog, 1995, p.379]

- Identify what knowledge assets an organization possesses.
    - Where is the knowledge asset?
    - What does it contain?
    - What is its use?
    - What form is it in?
    - How accessible is it?

- Analyzing how the knowledge can add value.
    - What are the opportunities for using the knowledge asset?
    - What would be the effect of its use?
    - What are the current obstacles to its use?
    - What would be its increased value to the company?

- Specifying what actions are necessary to achieve better usability and added value.
    - How to plan the actions to use the knowledge asset?
    - How to enact actions?
    - How to monitor actions?

- Reviewing the use of the knowledge to ensure added value.
    - Did the use of it produce the desired added value?
    - How can the knowledge asset be maintained for this use?
    - Did the use create new opportunities?

3. Knowledge Types

There are three classes of knowledge: tacit knowledge, rule-based knowledge, and background knowledge. An organization must adopt a holistic approach to knowledge management that combines all three knowledge types at all levels of the organization.

Tacit knowledge is the hands-on experience and specialty skills that individuals attain through their every day working activities. The following example explains tacit knowledge: "The skilled carpenter knows just how a given variety of wood must be handled, or what type of joint will best serve his purpose at a particular edge. To say that he 'knows' these things is not to say that he could put his knowledge into words. That is never entirely possible...the practitioner's knowledge of the medium is tacit. It is essential to skilled practice: the carpenter uses what he knows with every stroke of his tool." [Zuboff, 1988, p187] In this example the carpenter has gained his knowledge of woodwork through hands-on experience and on-the-job training. Tacit knowledge, see Table 1, promulgates task effectiveness within an organization.

The flipside to tacit knowledge is explicit knowledge. Explicit knowledge can be defined as the knowledge available to individuals through some type of information storage system. Unlike tacit knowledge, where an individual knows something due to his or her experience, explicit knowledge is based on the storing of the experiences of others. Explicit knowledge links the individual to the reusable codified knowledge through databases and electronic libraries. These two approaches to knowledge are further described in Figure 34.

These two types of knowledge, explicit and tacit, are described in depth by the knowledge theorists Ikujiro Nonaka and Hirotaka Takeuchi in their book The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. An excerpt from their book is provided below.

> Although Western managers have been accustomed to dealing with explicit knowledge, the recognition of tacit knowledge and its importance has a number of crucially relevant implications. First, it gives rise to a whole different view of the organization-not as a machine for processing information but as a living organism. Within this context, sharing an understanding of what the company stands for, where it is going, what kind of a world it wants to live in, and how to make that world a reality becomes much more crucial than processing objective information. Highly subjective insights, intuitions, and hunches are an integral part of knowledge. Knowledge also embraces ideals, values, and emotion as well as images and symbols. These soft and qualitative elements are crucial to an understanding of the Japanese view of knowledge. [Nonaka and Takeuchi, 1995, p.9]

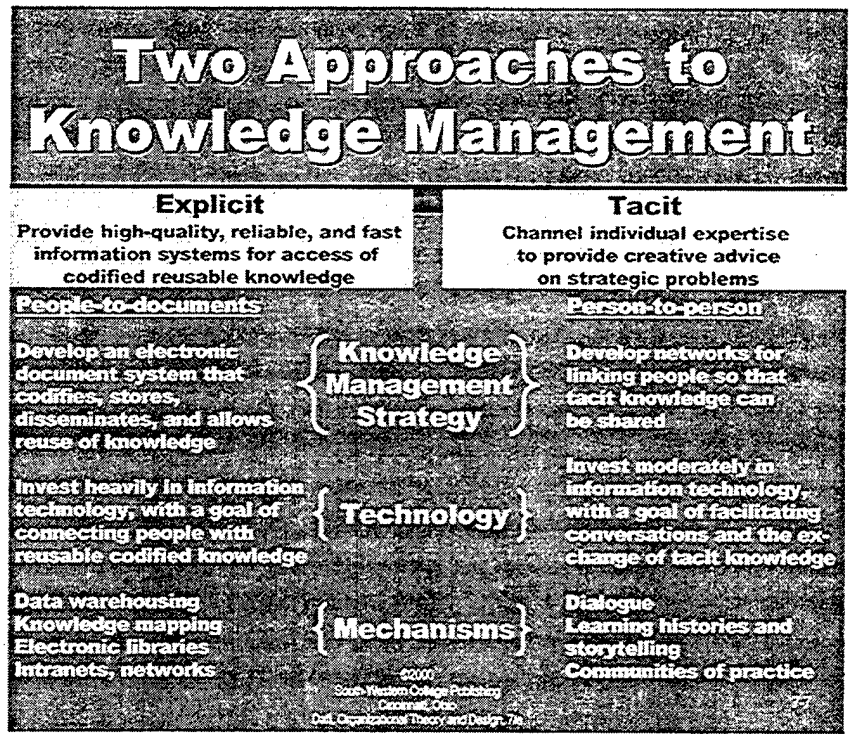

Figure 34. Approaches to Knowledge Management [From: Nixon, 2000]

Rule-based knowledge is knowledge that involves matching certain preformatted rules to various situations. Rule-based knowledge guides an individual's actions by answering three questions: What kind of situation is this? What kind of organization is this? And what does this particular organization do in this situation? This type of knowledge is very common in design standard operating procedures and organizational routines, and enables an organization to maintain a certain level of efficiency and control. [Choo, 1998]

Background knowledge supplies the mindset or worldview by which people in the organization understand particular events, actions, or situations in distinctive ways. [Morgan 1986] Background knowledge, see Table 16, promotes organizational

commitment from its individuals by uniting them under common views and beliefs. An example of this would be the certain views that one sports team would hold for its competitors. If a player were newly acquired he would assume the same views of his teammates in a relatively short time about their competitors.

Type	*Form*	*Example*	*Use*
Tacit Knowledge	-Procedural -Embedded in action	-Know how -Heuristics -Intuitions	-Ensures task effectiveness
Rule-Based Knowledge	-Declarative -Encoded in programs	-Routines -Standard Operating procedures	-Promotes operational efficiency and control
Background Knowledge	-Contextual -Expressed in texts	-Stories/metaphors -Mindsets/world views Visions/scenarios	-Instills commitment through shared meanings

Table 16. Knowledge Management Table [After: Choo, 1998]

Organizations are quickly coming to view knowledge as one of, it not the most important strategic resource for success. Along those same lines, organizations must understand the most productive way that knowledge can be utilized in problem solving and decision-making. An organization must continuously review, expand, and revise its knowledge base in all three of these categories in order to maintain its overall efficiency and effectiveness. Technical and organizational initiatives, if integrated correctly, will provide a comprehensive infrastructure to support the knowledge management process and in turn support organizational success. [Zack, 1999, p.125]

E. CONCLUSION

Organizations are tools that are designed to accomplish prescribed goals and milestones. [Perrow, 1972, p.180] The organizational design characteristics and factors described in this chapter play an integral part in the success of any organization, no matter the size, strategy or environment. A second point brought out in this chapter is the importance of the organization's process flow of information and the development/usability of knowledge and understanding. This is illustrated in Figure 32, the Cognitive Hierarchy of information processing. What is successful for an organization today may not be successful tomorrow. Therefore, organizations must come to the realization that they must adapt to the existing environment, and in order to accomplish this adaptation they must be willing to innovate, both strategically and organizationally.

The basic definition of any organization is that it is " a consciously coordinated social entity, with a relatively identifiable boundary, which functions on a relatively continuously basis to achieve a common goal or a set of goals." [Robbins, 1990, p.4] Organizations vary in structure, size, environment, and purpose, but the underlying fact that makes all organizations similar is that they are together to achieve a relatively common goal or end state. Of course the individuals within any organization will have their own personal motivations and goals, but the culmination of the achievement of those personal goals will inevitably lead to overall organizational prosperity. Charles Perrow accurately describes the issue of organizational goals in his book Complex

Organizations: A Critical Essay. Perrow states "....goals are set by the leaders and then broken down into sub-goals at each level of the organization. Each lower-order goal becomes a means to a high-order goal. People do not accept these goals because they necessarily share them or believe in them, but because the organization has mechanisms to insure that working toward them meets the individuals own personal values." [Perrow, 1972, p.150] Therefore, organizational success is relatively dependent upon the success of the individuals within that organization.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. STRUCTURE FOR THE INFORMATION OPERATIONS COUNCIL (IOC)

> For U.S. policy, an early implication of our work is that counter-netwar will require very effective interagency operations, which by their very nature involve networked structures. It should not be necessary, or desirable, to replace all hierarchies with networks. Rather, the challenge will be to blend these two forms skillfully, while retaining enough central authority to encourage and enforce adherence to truly networked processes. In this manner, states may come to be better prepared to confront the multitude of new threats emerging in this information age. [Arquilla and Ronfeldt, 1997, p.291]

A. STRUCTURAL OVERVIEW

1. Introduction

The proposed organization would be titled the Information Operations Council (IOC) and its primary goal is to ensure that all relevant departments and agencies play their appropriate role in the formulation and implementation of both foreign and domestic Information Operations policy. This council would be headed by a National Chief Information Officer (NCIO), who would be directly appointed by the President and retain a position on the National Security Council.

The reason for appointing an official at this high level is because of the need for a fully integrated inter-agency Information Operations Council that possesses the ability to incorporate IO policy and doctrine into National Security. The current IO picture does not delineate a specific entity who; (1) has the sufficient authority and (2) can directly oversee this task. The current IO organizational structure is insufficient. It is a

culmination of "individuals" from twenty-eight executive agencies that meet to develop recommendations for information technology management issues, procedures, and standards. The majority of these individuals have taken on the position of departmental Information Officers not as their primary job, but as a collateral tasking as was delineated in Chapter Three. This is extremely insufficient in this complex IO environment and is the equivalent of using a band-aid to stop the bleeding from a major wound. In essence, the short term problem may receive a temporary fix, but sooner than later the problems will have compounded tenfold. In today's uncertain world where, more often than not, identifying the enemy/adversary is becoming more and more difficult, Information Operations can no longer be thought of as a "part-time" job.

The empowering of the NCIO would ensure that not only recommendations were made, but that IO policy is implemented across agency boundaries and that potential problems are addressed in an efficient and effective manner.

2. Information Operations Council Configuration

The authors have proposed a hybrid configuration for the Information Operations Council. This hybrid configuration would be a combination of the divisional configuration and the matrix configuration.

The divisional configuration, a hierarchy, is characterized by subunits (e.g. Departmental CIO) within the organization that manage the tactical and operational activities. This enables the top management (e.g. NCIO) to focus on strategic planning and operations. The divisional configuration also facilitates improved coordination of

functional activities and allows for a fast adaptation to environmental and market changes.

The matrix configuration, a duel hierarchy, promotes interdepartmental cohesion and effective information distribution in the organization. This is an essential factor in developing a successful Information Operations Council. A second motive for choosing this configuration is because the matrix configuration "...assigns specialists from functional departments to work on one or more interdisciplinary teams." [Burton and Obel, 1998, p.45]

The integration of these two configurations will promote a high degree of departmental responsibility through the divisional configuration and at the same time drastically improve inter-departmental coordination and information distribution.

The proposed Information Operations Council will be comprised of one National Chief Information Officer (NCIO), one Deputy NCIO for Foreign Affair, one Deputy NCIO for Domestic Affairs, and seventeen Chief Information Officers representing the departments/agencies identified and described in Chapter Three. (See Figure 35.) Although these members are representatives of their perspective departments, they must be place the needs and requirements of the IOC on the same level, if not on a higher level than those of their departments.. This is a situation that will undoubtedly be met with enormous resistance, which is another reason why the position of the NCIO must be an Executive appointee who is given enough authority and control to carry out agenda and accomplish the goals of the IOC.

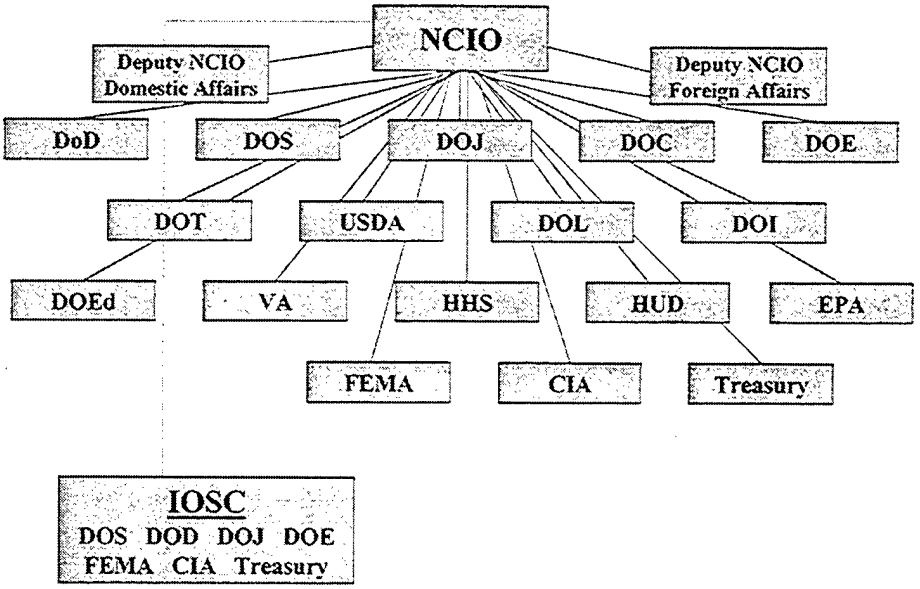

Figure 35. Organizational Structure of IOC

B. DEFINING MAJOR PLAYERS AND RESPONSIBILITIES

1. National Chief Information Officer

The National Chief Information Officer is designated by the Executive Branch of government, and is responsible for establishing and maintaining a national Information Operations doctrine and strategic plan. The NCIO's duties will include enforcing inter-agency IO structure, the development and implementation of doctrine and policy with the intent of maintaining a comprehensive operating picture of the IO environment. This position will be required to play an innovative role in informational aspects of National

Security policy and planning, and to not only focus on the "now," but to look beyond and define a larger IO environment.

The NCIO will be required to maintain a bold leadership style while possessing the attributes of a visionary, who is willing and able to set a new course for the way business is done in the IO environment. He must have the ability to see IO situations for what they are and to report frankly, and without hesitation, to the President on matters regarding Information Operations. Without his strong leadership and the support from the President, this organization will never accomplish its demanding goals and will falter in the realm of Information Operations and National Security.

2. Deputy NCIO for Foreign Affairs

The Deputy NCIO for Foreign Affairs is the primary assistant to the NCIO on IO matters that originate from outside the United States, or that effect foreign relations. This deputy would have a close working relationship with NCIO and the departmental/agency CIOs as to coordinate a common IO picture in the area of foreign relations. The relationship between the Deputy NCIO for Foreign Affairs and the Department of State will play a significant role in the development of, and constant adjustment of foreign policy. A second integral relationship will be that of the Deputy NCIO for Foreign Affairs and the CIO for the Central Intelligence Agency. These two actors must be forthright with their information in order to maintain a common informational operating picture in the global environment.

3. Deputy NCIO for Domestic Affairs

The Deputy NCIO for Domestic Affairs is the primary assistant to the NCIO on matters that originate from inside the U.S. or that effect the domestic infrastructure. This deputy would have a close working relationship with NCIO and the departmental/agency CIOs as to coordinate a common IO picture in the area of domestic Information Operations.

4. Departmental / Agency CIOs

Their respective Secretaries designate an executive agency's CIO. As their agency's CIO, they would be responsible the oversight of all Information Operations within their department. Although their respective Secretary/Director appoints them, they also will be directly responsible to the National Chief Information Officer for the implementation and promulgation of all Information Operations policy and doctrine.

5. Support Staff

The individual members of the council would assemble their respective support staffs. These staffers would work closely with their respective CIO to ensure that they are current on issues directly and indirectly related to their area of responsibility. Again, these positions cannot be filled as "collateral" jobs. The individuals employed by the IOC must work for the IOC and their CIO only. The days of "part-time" IO must come to an end. An added advantage to this approach is that the support staff is getting direct

exposure to the IO environment, thus receiving "indirect on-the-job training" (tacit knowledge).

C. DELINEATING ORGANIZATIONAL RELATIONSHIPS

1. NCIO and CIOs

The NCIO would work weekly and as required with the CIOs. The purpose of these frequent meetings is to further advance the role and effectiveness of the IOC. The weekly meetings would entail discussions of new policies, current and future threats, and any other aspects of IO.

2. NCIO to Deputy NCIOs

The NCIO would work day to day with the deputies to ensure that there is a coherent operating picture in IO. This relationship is important to ensure that the blending of domestic and foreign IO is seamless where required.

3. Deputy NCIOs to CIOs

The deputy NCIOs would meet weekly and as required with the CIOs to ensure that each executive agency is in tune with the entire IO orchestra, both foreign and domestic.

4. CIO to CIO

The CIOs should operate independently except when meeting weekly with the council or as necessary. The CIOs will interact with the NCIO, the deputies and each other to share ideas ensuring that all IO assets are being effectively allocated.

5. CIO to Support Staff

The staff would be tasked according to the priorities of their CIO. Staff members would include experts, technicians and analysts in the Information Operations field relating to their respective executive agency.

D. THE INFORMATION OPERATIONS SECURITY COUNCIL (IOSC)

The Information Operations Security Council (which could quite possibly merit a separate research topic of its own) will become an integral entity in defining the National Security Strategy of the United States in the very near future. This topic, U.S. National Security, has been previously discussed in Chapter Four. The IOSC, illustrated in Figure 35, would be comprised of "mandatory" members from the following department/agencies:

- Department of State
- Department of Defense
- Department of Justice
- Department of Energy

- Department of Treasury
- Department of Transportation
- Federal Emergency Management
- Central Intelligence Agency

At times the NCIO may be inclined to bring in other members of the Information Operations Council as "advisory" members. This would be done in a similar fashion to the way the President brings in advisory members for the National Security Council.

The IOSC would be similar to, if not the actual, CIA Intelligence Community (IC). The purpose of this sub-council within the IOC would be to ensure that those IO issues effecting national security are given special attention. The executive agencies that contribute to the national security of the United States would be permanent members of the IOSC. These agencies include: Defense, State, Treasury, Justice, Energy, CIA and FEMA. Other members of the IOC may be called upon to meet with the IOSC, as the situation arises, to discuss national security threats or issues that pertain to that IOC member's realm. An example of this is discussed in Chapter Four.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. ANALYSIS OF INFORMATION OPERATIONS COUNCIL

A. OVERVIEW OF ORGANIZATIONAL CONSULTANT

1. Introduction

Organizational Consultant is a decision support tool that makes educated recommendations on organizational structure. These recommendations are dependent upon the user's inputs. Some of the inputs will be based on observations and others will be based on judgment. The output from Organizational Consultant is composed of the recommended improvements and the organization's situational misfits. The recommended improvements are self-explanatory. The misfits are basically combinations of certain situations or attributes within the organization, which can lead to lower organizational performance. Situational misfits are detractors in organizational design and structure that prevent the organization from reaching its full potential.

The Input categories in Organizational Consultant are made up of the following: current configuration, current complexity, current formalization, current centralization, size, age/ownership, diversity, technology, environment, management profile, strategy factors, and climate factors. Theses categories are comprised of between one to ten questions that inquire specifics about the organization. If one of the questions is not applicable to the organization the user has the option to choose the "no answer" choice. Also, with each question there is a "certainty factor." This certainty factor allows the user

to indicate the degree of certainty for that specific input. This allows the Organizational Consultant to evaluate each question appropriately and with the accurate level of importance. The range for the certainty factor is between –100 and 100. Through the user's answers to these questions the organization is then defined.

2. Fit Criteria

Fit is an organizing concept that is used to develop a knowledge base. "Fit suggests a synthesis and integration of concepts to create definitions. The challenge is to create a knowledge base system that utilizes known theory for a given situation to suggest appropriate organizational design recommendations. To meet these goals the knowledge base must fit together across a number of dimensions." [Burton and Obel, 1998, p.15]

There are four fundamental criteria that are needed for a functional organization. These criteria are:

- **Contingency Fit:** The Contingency fit is dependent upon there being a good fit between the contingency factors of the organizational structure (e.g. Management style, Climate, Size, Environment, Technology, Strategy) and the design parameters of the organization (e.g. Complexity, Formalization, Rules, Reports, Communications). This relationship can be seen in Figure 36. "The contingency fit criteria can largely be achieved through careful attention to the contingency theory literature and translation of that knowledge into appropriate if-then statements." [Burton and Obel, 1998, p.17]

- **Situational Fit:** Situational fit is determined by whether or not the organization's "situational facts" make sense. For example, the organization's management style must fit the environment; if one were to change then the other must also change in order to maintain a situation fit. It is basically a

matter of consistency within the organizational structure. "The control of situational fits and misfits is a key to organizational success." [Burton and Obel, 1998, p.17]

- **Design Parameter Fit:** Design fit is characterized as a fit between the properties of an organization's design parameters (e.g. Centralization, Complexity, Formalization), seen on the right side of Figure 36, and the organization's contingency factors (e.g. Management Style, Size, Technology), seen on the left side of Figure 36. The difficulty in attaining a design parameter fit is in balancing the recommendations. "For example, a design recommendation that the organization should be decentralized can be driven by a number of contingencies. Management style, climate, size, environment, technology, and strategy all may suggest decentralization. However, the more likely situation is that there are design propositions that suggest decentralization and others that suggest centralization." [Burton and Obel, 1998, p.17]

- **Total Design Fit:** The Total fit is the culmination of the above-mentioned fits (Contingency, Situational, and Design). Obviously, this is the most difficult fit to attain because it requires that not only must the design recommendations fit internally to the organization, but they must also fit the actual situation. If serious situational misfits are present, and not corrected then the total design fit will be impossible to obtain.

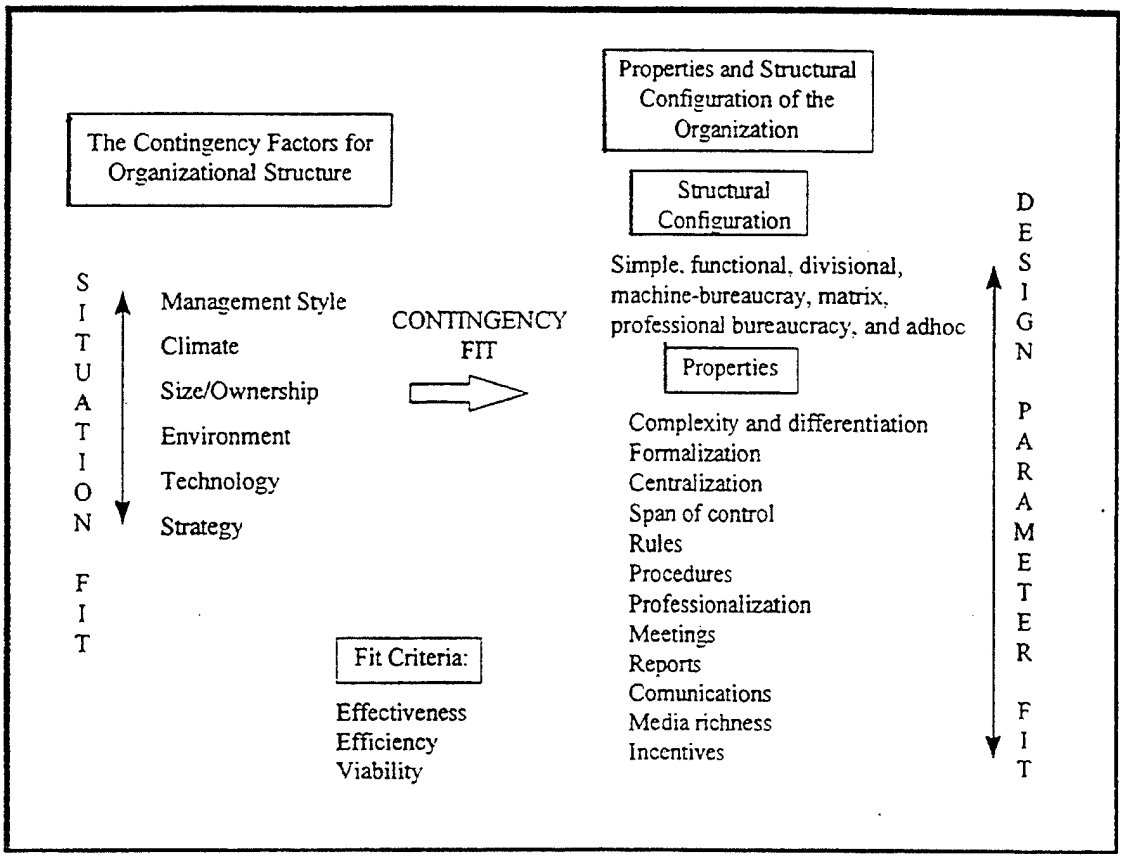

Figure 36. Contingency Theory - Organizational Design Fit [From: Burton and Obel, 1998]

In this scenario the organization is a new proposal, so some of the answers to the Organizational Consultant questions will be conceptual in nature.

B. INPUTS TO ORGCON

1. Current Configuration

An organization's configuration is basically its chain of command. It specifies who is responsible for what tasks within the organization. There are seven basic

stereotypical organizational configurations: simple, functional, divisional, matrix, machine bureaucracy, professional bureaucracy, and ad hoc. An organization is not always one of the above-mentioned stereotypical configurations. Many times an organization can possess attributes of one or more of these and in many situations those "hybrid" configurations are very adaptive and in turn very successful.

The Inter-agency Information Operations organization proposed in this research will possess attributes of three of the above-mentioned configurations. In order for the organization to flourish it should possess attributes from the following configurations:

- The Information Operations Council will be predominately comprised of a divisional configuration. This configuration will best fit this organization because it will allow the each individual Departmental Chief Information Officer to handle the day-to-day operations and tactical issues and at the same time allowing the National Chief Information Officer to focus his efforts on the strategic issues. However, the draw back to this configuration is that it sometimes tends to promote autonomy and minimizes interdependency between the individual units. This could cause redundancy and "stove-piping" within the organization.

- The Information Operations Council should also possess attributes of a matrix configuration in order to promote interdepartmental cohesion and effective information distribution. The matrix configuration "...assigns specialists from functional departments to work on one or more interdisciplinary teams." [Burton and Obel, 1998, p.45] The matrix configuration focuses on making required adjustments in the organization and managing uncertainty. The goal of the matrix configuration is to "capture the effectiveness of the division as well as the efficiency of the functional configuration under uncertainty." [Burton and Obel, 1998, p.64] This is an important concept that the Information Operations Council must fully comprehend.

- Lastly, there will be elements of the machine bureaucracy configuration present in the Information Operations Council. These elements are inevitable, any governmental organization will possess a proper chain of command and will be highly formalized with rules and regulations. And lastly government organizations tend to have a well-defined hierarchy. Although some of these attributes will be somewhat inevitable the authors contest the belief that because the organization is within the government that it is obliged to follow a configuration of a machine bureaucracy. A strict machine bureaucracy will only defeat the purpose of the Information Operations Council, which is to break down the common barriers/walls that currently exist between departments in the information operations environment.

Although there are elements of each of these configurations in the Information Operations Council, a mixture or "hybrid" configuration that combines the divisional and matrix configurations, while minimizing the effects of the inevitable machine bureaucracy, will be best suited to accomplish organizational goals. Unfortunately, the authors have been limited to only one choice for the current configuration question in Organizational Consult. The authors have chosen the divisional configuration because this configuration is the best fit.

2. Current Complexity

The amount of horizontal, vertical and spatial differentiation within an organization defines its degree of complexity. The horizontal differentiation is defined as the varying amounts of specialization within the organization. The depth of the organization's hierarchy or chain of command determines an organization's vertical differentiation. Spatial differentiation can simply be described as the extent that an

organization is geographically spread out. [Burton and Obel, 1998, p.68] For instance, is the organization global, international, national, or regional? The proposed Inter-Agency IO organization is moderately complex, in that there are numerous departments/agencies that are involved. There will be a high need for detailed coordination between these separate departments, which is why each departments will be required to have their own departmental Chief Information Officer. Geographic complexity will not be overly important because each of the departmental CIOs will be located within the organization's main center. Vertical levels will number between three and five, and all of the roles will require advanced degrees.

3. Current Formalization

Formalization can be explained as the basic rule and regulations of an organization. These rules could range from working hours and attire to standards and procedures for executing a deal or orders. "We measure formalization as the degree to which there exists formally stated rules, in writing." [Burton and Obel, 1998, p.73] The degree of formalization could vary at different levels of any organizations. In many instances an organization will be extremely formalized at its lower levels where direction and supervision are needed, but at upper levels formalization is replaced by experience and knowledge. The Inter-agency IO organization should have a level of medium formalization, but will most likely be highly formalized, if for no other reason than because it is a governmental organization. The majority of the rules and procedures will be in writing. The difficulty this organization will face will be trying to adhere to this

level of formalization while continuously dealing with a very uncertain environment and trying to adapt to these uncertainties. Senior leadership must be able to have some latitude in their decision making process.

4. Current Centralization

Centralization, in its simplest form can be explained as to what extent upper management is involved in the overall operations of an organization. A few questions that should be asked in order to determine an organizations level of centralization: Are the decision makers involved in the day-to-day intricacies of the organization? To what extent is the decision making process delegated? Is authority delegated or does it rest at the top? We measure centralization by how much direct involvement top managers have in gathering and interpreting the information they use in decision-making and the degree to which top management directly controls the execution of a decision [Burton and Obel, 1998, p.75]. The proposed IO organization will be highly centralized at the upper levels (e.g. National Chief Information Officer, National Security Council), but somewhat decentralized at the separate department levels. Upper leadership will have direct control over the implementation of policy and the execution of decisions.

5. Size

The size of an organization is defined by the obvious: the number of individuals within an organization. The greater the number of people the larger the organization. The skill levels of individuals determine the number of people required. An organization with

highly trained and skilled individuals tends to behave larger than an organization with the same number of unskilled individuals. Thus, the employee number is factored up to reflect this difference. Size is used here as a measure of the information processing capacity. A larger organization requires greater information processing capacity. The education and skill level of the employees is important in this respect. [ORGCON, 1998]

In the case of the IO organization, although the overall organizational size will be greater than 2,000 individuals, the authors will only be examining the organization from the upper-middle management levels and higher.

6. Age/Ownership

Age in an organization varies throughout the different organizational levels, there are certain organizations where age is limited within a certain age group. In the Inter-agency IO organization the authors will be focusing on the middle to upper management, therefore the age will not vary as much. The ownership is obviously going to be government.

7. Diversity

Organizational diversity pertains to the different types to diversity of products and services that an organization provides. "A greater number of products indicates a greater variety in the organization's activities and is a measure of differentiation. The exact number is less important than the perception of the variety or differences among the products." [ORGCON, 1998] Although the Inter-agency Information Operations

organization's prime service/product is information, the types of information will greatly fluctuate. Because of this fluctuation, the organization is considered highly diversified.

8. Technology

Technology is considered to be the equipment, and methods used by an organization to achieve its goals. Technology often is considered to be the key to an organization's success. Unfortunately, this is a misconception. Technology is only a part of what is required for an organization's success and could even be detrimental to an organization if it is not utilized correctly. The Information Operations Council will have to us advanced information systems for proper command and control.

9. Environment

An organization's environment is defined as the arena in which the organization operates. "The environment consists of many different parts. The industry, including its size and competitions, is a major part of the organization's environment." [Burton and Obel, 1998, p.201] The environment also includes, but is not limited to, suppliers, politics, customer bases, finances, and social attitudes. The level of uncertainty in the information operations environment is very high, which in turn produces a very complex and competitive environment.

10. Management Profile

An organization's management profile is basically the leadership style of the upper management/decision makers. The management profile must be a good fit with the organizational structure. If it is not a good fit then the organization will not achieve its goals. Senior leadership will make the majority of policy and general decisions for both the long and short term, while operating decisions will be made at the separate departmental levels. The top management in the Information Operations Council has to be extremely proactive in its' thinking in order to stave off potential IO threats.

11. Strategy Factors

An organization's strategy is one of the essential determinants of organizational design. It determines what the organization's long term goals and milestones will be. An organization's strategy and structure must fit together in order for the organization to achieve those goals and milestones. This organization will possess a high capital requirement and be highly innovative in doctrine/policy matters. The organization's concern for quality will be exceedingly high.

12. Climate Factors

The organizational climate refers to the beliefs and attitudes held by individuals about their organization. The climate is a relatively enduring quality of an organization that (1) is experienced by employees, and (2) influences their behavior. [ORGCON,

1998] The Information Operations Council must have a high level of trust if the council is to succeed. This also will be difficult to achieve because of the departmental walls/barriers that are presently in existence. Information assurance and security must be a chief concern for all members in the council, as this is becoming more and more difficult to control.

C. RESULTS FROM ORGCON

As discussed previously in this chapter, Organizational Consultant is a decision support tool that diagnoses organizational problems and makes educated recommendations on organizational structure. As described by Burton and Obel in Strategic Organizational Diagnosis and Design, "....Organizational Consultant is an expert/knowledge base system, which incorporate knowledge derived from experts into an information processing framework for organizational design. This knowledge base has been transformed into a system of decision rules." [Burton and Obel, 1998, p.347] Organizational Consultant will analyze the organization based on the inputs of the user, and upon the completion of that analysis the program will produce a detailed report. The explanations provided in the report summary relate the specific recommendations and conclusions to the organizational design theory. It is important to understand that the answers provided through the report summary are not the "all and end all" for the most successful organizational design. These conclusions and recommendations are only biased because they are generated in the decision support system and based on the inputs of the individual and their understanding/interpretation of the organization. [Burton and

Obel, 1998, p.348] Additionally, the decision support system rules are empirically validated only for business scenarios.

The individual input questions and answers can be found in Appendix A and the detailed results from Organizational Consultant can be found in Appendix B.

1. Size

The size of the organization - large, medium, or small - is based upon the number of employees, adjusted for their level of education or technical skills. [ORGCON, 1998]

The size of the Information Operations Council has been deemed medium by the authors. It is also more than likely that all members of this council, since they will also be upper-management officials within their perspective departments/agencies, will possess some type of higher education.

> Based on the answers...provided, it is most likely that your organization's size is medium (cf 80). More than 75 % of the people employed by IOC have a high level of education. Adjustments are made to this effect. The adjusted number of employees is lower than 1,000 but greater than 500 and IOC is categorized as having a medium size. [ORGCON, 1998]

2. Climate

The organizational climate effect is the summary measure of people and behavior. [ORGCON, 1998] The beliefs, attitudes, and perspectives of the individuals within the organization determine the organization's climate. The organizational climate can be further defined as "the relatively endearing quality of the internal environment of an

organization that a) is experienced by its members, b) influences their behavior, and c) can be described in terms of the values of a particular set of characteristics (attitudes) of the organization." [Taguiri and Litwin, 1968, p.27]

> Based on the answers...provided, it is most likely that the organizational climate is a developmental climate (cf 64). The developmental climate is characterized as a dynamic, entrepreneurial and creative place to work. People stick their necks out and take risks. The leaders are considered to be innovators and risk takers. The glue that holds organizations together is commitment to experimentation and innovation. The emphasis is on being on the leading edge. Readiness for change and meeting new challenges are important. The organization's long-term emphasis is on growth and acquiring new resources. Success means having unique and new products or services and being a product or service leader is important. The organization encourages individual initiative and freedom.
>
> Medium to high leader credibility characterizes an organization with a developmental climate. When the organization has a high to medium level of trust it is likely that the organization has a developmental climate. Employees with a high morale is frequently one element of a developmental climate. An organization with a medium level of scapegoating may have a developmental climate. [ORGCON, 1998]

3. Management Style

An organization's management style can have a vast effect on how the organizational structure is formed and if/how it will evolve. At the same time it is quite possible for management to adapt to the existing structure. The key to a successful management – structure relationship is to ensure that there is a good fit between the two.

The level of management's micro involvement in decision-making is the summary measure of management style. Leaders have a low preference for micro involvement; managers have a high preference for micro-involvement. [ORGCON, 1998]

Organizational Consultant made the following observations in reference to the Information Operations Council's climate:

> Based on the answers...provided, it is most likely that your management profile has a medium preference for micro involvement (cf 73). Management has both a short-term and long-term horizon when making decisions, which characterizes a preference for a medium micro involvement. Management is risk neutral. This is one of the characteristics of a manager with a medium preference for micro involvement. Since the management has a preference for medium detailed information when making decisions a medium preference for micro involvement characterization is appropriate. Management has a preference for using both motivation and control to coordinate the activities, which leads toward a medium preference for micro involvement. [ORGCON, 1998]

4. Strategy

"Structure follows strategy or strategy follows structure," this debate has been going on for quite some time. Amburgey and Dacin [1994] argue that strategy is more important in determining structure than structure is in determining strategy. Whichever is the case, in the end the most important factor will be whether or not there is a sufficient fit between the two, "The fit between strategy and organizational structure has crucial implications for the performance of the organization." [Miller, 1987b]

The organization's strategy is categorized as one of either prospector, analyzer with innovation, analyzer without innovation, defender, or reactor. These categories follow Miles and Snow's typology. Based on the authors' inputs, the organization has been assigned to a strategy category. This is a statement of the current strategy; it is not an analysis of what is the best or preferred strategy for the organization. [ORGCON,

1998] The preferred strategy will be discussed in the recommendations section later in this chapter.

Organizational Consultant found that it is most likely that the IOC's organizational strategy is that of an analyzer with innovation strategy, with a certainty factor of 68%. It also states the strategy could also be that of a prospector, with a certainty factor of 65%. An organization with an analyzer with innovation strategy is an organization that combines the strategy of the defender and the prospector. It moves into the production of a new product or enters a new market after viability has been shown. But in contrast to an analyzer without innovation, it has innovations that run concurrently with the regular production and it has a dual technology core. [ORGCON, 1998] Organizational Consultant states the following:

> With a concern for high quality an analyzer with innovation strategy is a likely strategy for IOC. With top management preferring a medium level of micro involvement top management wants some influence. This can be obtained via control over current operations. Product innovation should be less controlled. The strategy is therefore likely to be analyzer with innovation. For a medium routine technology, IOC has some flexibility. It is consistent with an analyzer with innovation strategy. [ORGCON, 1998]

A prospector is constantly seeking new product opportunities to serve the existing and potentially new customers. With a concern for high quality a prospector strategy is a likely strategy for IOC. For a prospector strategy to be aggressive in product development or market opportunities exploitation, it requires a high capital investment. An organization with a prospector strategy is an organization that continually searches for market opportunities and regularly experiments with potential responses to emerging environmental trends. Thus, the organization is often the creator of change and

uncertainty to which its competitors must respond. However, because of its strong concern for product and market innovation, a prospector usually is not completely efficient.

The Information Operations Council must possess traits of both the analyzer with innovation, and the prospector strategies. So in essence the organization will possess a hybrid strategy that combines the two in order to meet the challenges of the uncertain environment.

5. Current Organizational Characteristics

Based on the authors' inputs, the organization's complexity, formalization, and centralization have been calculated. The current organization has been categorized with respect to formalization, centralization, and complexity. The categorization is based on the input given and does not take missing information into account. This is the current organization. Later in this chapter, there will be recommendations for the organization. Below are the current organizational characteristics:

- The current organizational complexity is medium (cf 75).
- The current horizontal differentiation is high (cf 80).
- The current vertical differentiation is low (cf 70).
- The current spatial differentiation is low (cf 70).
- The current centralization is medium (cf 86).
- The current formalization is high (cf 70).

D. MISFITS

Organizational Consultant provides two types of misfits in its report summary. These misfits are called situational misfits and organizational (design parameter) misfits. The situational misfit occurs when there are internal inconsistencies within the organization's design situation. "Situation misfits may appear due to changes in the environment and thus be exogenous to the organization. Misfits may also appear because of management decisions." [Burton and Obel, 1998, p.17] If Organizational Consultant finds that an organization does not have any situational misfits then it is assumed that there is a high level of internal consistency within the organizational structure. Situational misfits must be controlled if the organization is going to be successful.

Organizational misfits, also called design parameter misfits, exist when the existing level of the organization's design parameters differ from those recommended by Organizational Consultant. [Burton and Obel, 1998, p.392] Organizational misfits will be evident when the "if-then" propositions, used in the determination of the organization's design, are not met and hence are unbalanced.

1. Situational Misfits

A situation misfit is an unbalanced situation among the contingency factors of management style, size, environment, technology, climate, and strategy. [ORGCON, 1998] Organizational Consultant has found that the following situational misfits are present, with a certainty factor of 100%:

> IOC has a high capital requirement but is not a large organization. The organization can be vulnerable. An organization with a high capital requirement and a few employees usually makes a few standardized products. Further, the technology is likely to be very limited in adaptiveness. The organization is then vulnerable to changes in the environment, market and products changes. Smaller organizations with small capital requirements are frequently more adaptive. To reduce this vulnerability, the organization should consider creating a greater capability for adaptation, which will usually require more employees of higher skill, education and training. [ORGCON, 1998]

The above-mentioned situational misfits are mostly due to the manner in which the authors have "bound" the proposed organization. The authors specifically bound the problem by concentrating on the upper management level of the Information Operations Council. This ultimately affects the size and complexity of the organization, which in turn causes a situational misfit between organizational size and capital requirement. Also, Organizational Consultant correlates small organizations that have high capital requirements with the production of few standardized products. The authors consider the products of the IOC to be countless. Although information can be considered one product, the realm of information operations is practically infinite and knows no bounds.

2. Organizational Misfits

Organizational (Design Parameter) misfits compare the recommended organization with the current organization. [ORGCON, 1998] The current organization is the direct result of the user's input to, or in other words how the user interprets the

organization. The prescribed organization is defined as the best recommended fit for the organization, through Organizational Consultant's decision support system rules. Organizational Consultant has found that only one organizational misfit is present, with a certainty factor of 100%:

- Current and prescribed formalization do not match.

This is somewhat of a positive outcome for the basic design/structure of the proposed Information Operations Council. The authors specifically answered the majority of the formalization questions in Organizational Consultant to the "highly formalized" side. Formalization is a fact of life in government organizations and is something that needs to be addressed in the future.

The basic reasoning behind this misfit is that the excessive formalization will stifle innovation and the proverbial "out of the box" thinking, which are essential to success in the IO realm. Some even go to the extent of deeming this environment as the "Information Revolution", but these are the same people that try to formalize or "do business like they always have in the past." How can one formalize something so new? This is where much of the problem lies today in governmental organizations. Excessive formalization tends to lead one to assume that "what worked today will work tomorrow and the next day," but this is certainly not always the case. This is not to say that there is no need for any formalization in organizational structure, just that future success in this environment will more dependent on innovation and forward thinking, and much less dependent upon formalization.

E. ORGCON RECOMMENDATIONS

Based on the authors' inputs about the organization, its situation, and the conclusions with the greatest certainty factor from the analyses above Organizational Consultant has derived recommendations for the organization's configuration, complexity, formalization, and centralization. There are also recommendations for coordination and control, the appropriate media richness for communications, and incentives. More detailed recommendations for possible changes in the current organization are also provided. [ORGCON, 1998]

1. Organizational Configurations

Organizational Consultant has determined that the configuration that best fits the situation has been estimated to be a divisional configuration, with a certainty factor of 69%. The following is the reasoning for Organizational Consultant's recommendation:

> A divisional organization is an organization with self-contained unit grouping into relatively autonomous units coordinated by a headquarters, (product, customer, or geographical grouping). When the organization is of medium size, the configuration can be a divisional configuration. Because the organization has many products, the configuration should be divisional. The configuration should be divisional when the equivocality of IOC's environment is not high and the complexity is not low. The divisionalization of IOC may be based on products or product groups. The divisionalization of IOC may be based on markets. The divisional configuration may be a multi-domestic structure. Because the technology is not fully divisible, care should be taken in recommending a divisional configuration. [ORGCON, 1998]

Organizational Consultant further added that the machine bureaucracy would most likely be the worst fit for the IOC. The basis for Organizational Consultant's observation

that a machine bureaucracy would be an ill suited configuration for the Information Operations Council is that the environment is highly hostile and uncertain. And that in this type of environment a machine bureaucracy would prevent the organization from acting appropriately when unexpected events occur.

Although the recommendation stated above coincides with the recommendation of the authors, there is still no definite configuration. While not a viable option in Organizational Consultant, the authors believe that the ideal configuration would be one that combines the key elements of the divisional and matrix configurations, while minimizing the effects of the inevitable machine bureaucracy. This configuration has been previously described as a "hybrid" configuration.

2. Organizational Characteristics

a. Complexity

Organizational complexity is the combination of vertical, horizontal and spatial differentiation. Horizontal differentiation is usually high when there are many small tasks to be accomplished that require individual specialization. The number of hierarchical levels within the organization determines vertical differentiation. Spatial differentiation is determined by the amount of different geographic locations the organization possesses. Lastly, complexity is also a by-product of the organization's preference for micro-involvement, size, environment, technology, and strategy. As the

organizational complexity becomes higher the demand for efficient information processing becomes higher and command and control becomes increasingly more difficult.

The IOC's horizontal differentiation is considered to be medium because of the fact that there are only a moderate number of different job titles. This is due to the fact that the authors "bounded" the organization to include only the separate Departmental Information Officers, the two Deputy Chief Information Officers, and the National Chief Information Officer. The vertical differentiation was also determined to be medium, again because of the way the organization has been bounded. There are only three to five levels that will separate the National Chief Information Officer (top) and the Departmental Information Officers (bottom). The spatial differentiation was deemed low due to the fact that the number of geographic locations separating the individuals is limited to the Washington D.C. area (less than 10 miles).

Organizational Consultant recommends that the degree of organizational complexity is medium for the Information Operations Council. The certainty factor associated with this recommendation was 62%. Organizational Consultant states that, for the most part, medium sized organizations should have medium complexity and that top management of IOC has a preference for a medium level of micro involvement, which drives the organizational complexity towards medium. This recommendation is explained in further detail below.

> IOC has a technology that is somewhat routine, which implies that the organizational complexity should be medium. The environmental

uncertainty of IOC is high, and the equivocality of IOC's environment is medium. For this situation the organizational complexity should be medium. There is no need for an elaborate hierarchy or work specialization. Because IOC has an advanced information system, organizational complexity can be greater than it could otherwise. A developmental climate in the organization requires a medium level of complexity. The recommended degree of horizontal differentiation is medium (cf 27). The recommended degree of vertical differentiation is medium (cf 48). It, too, could be: low (cf 44). [ORGCON, 1998]

b. Formalization

Formalization is defined as the rules, regulations, and standard operating procedures for an organization. "We measure formalization as the degree to which there exists formally stated rules, in writing." [Burton and Obel, 1998, p.73] It has also been stated that formalization can increase information processing capacity or decrease the demand for information processing. Formalization and configuration have direct effects upon one another, as seen previously in this chapter. For example, machine bureaucracy configurations will tend to be highly formalized, while matrix configurations will tend to be less bound by written rules and regulations.

As previously discussed, the authors answered the formalization questions from Organizational Consultant toward the highly formalized side. This in turn is what causes the only organizational/design parameter misfit. Organizational Consultant has recommended that degree of formalization be medium for the Information Operations Council. The certainty factor for this answer is 53%. Below is the explanation for this recommendation.

> There should be some formalization between the organizational units but less formalization within the units due to the high professionalization. Medium size organizations should have medium formalization. Organizations with medium-routine technology should have a medium formalization. Medium formalization is consistent with the leadership style when top management's preference for micro involvement is neither very great nor very low. [ORGCON, 1998]

c. Centralization

Centralization is measured by the amount of direct involvement top managers have in gathering and interpreting the information they use in decision-making and to what degree is the execution of a decision controlled by top management. Centralization has a direct relationship with the demand for information processing. As the demand for information processing rises, more individuals have to get involved in the decision-making process. This will lead to an increase in decentralizing the decision-making process within the organization.

Organizational Consultant has recommended that the level of centralization in the IOC be medium, but the detailed recommendation states reasons for the possibility of low, medium, and high centralization. It is evident to the authors that Organizational Consultant selected the "middle ground" for this category. The detailed recommendation is stated below.

> The recommended degree of centralization is medium (cf 59). IOC has an analyzer with innovation strategy. Centralization should be medium. There should be tight control over current activities and looser control over new ventures. When there is a high capital requirement and the product innovation is high, as is the case for IOC, centralization should be medium. IOC is of medium size. Such organizations should have medium to high centralization. Medium centralization is recommended when top

> management has neither a great desire nor very little desire for micro involvement. Because IOC has an advanced information system, centralization can be greater than it could otherwise. A developmental climate in the organization requires a medium to low level of centralization. [ORGCON, 1998]

d. Span of Control

Span of control is determined by how routine the technology is within an organization, and how important that technology is to the organization in their overall information a system. The Information Operations Council will be required to have dominant technologies and advanced information systems in order to effectively and efficiently accomplish their goals. This brings up the point made earlier about innovation and forward thinking. In order for the IOC to be effective, individuals must be continuously innovating, both doctrinally and technologically. The status quos will not work, information needs to be gotten to the right people at the right time and the only way to continuously accomplish this in the future is to increase the span of control through technological innovation.

Organizational Consultant has recommended that the IOC's span of control that is medium and the media required for use have a medium richness. Lastly, the IOC should an information media for a large amount of information.

> IOC's span of control should be moderate (cf 49). Since IOC has some technology routineness, it should have a moderate span of control. IOC should use media with medium media richness (cf 70). The information media that IOC uses should provide a large amount of information (cf 85). Incentives should be based on results (cf 85). [ORGCON, 1998]

e. Coordination and Control

"Coordination and control have two sides. One is to make sure that enough relevant information is available at the right time to be able to make the right decisions. The second is to make sure that the right decisions are made." [Burton and Obel, 1998, p.76] Command and control will play in integral role in the success of the proposed Information Operations Council. Coordination between the separate Departmental Chief Information Officers and the National Chief Information Officer will be imperative, for if the right information is not being properly and effectively distributed then it is not doing anyone any good. Organizational Consultant recommends that because the IOC's environment has medium equivocality, high uncertainty, and high complexity the command and control process promulgated through departmental meetings. A detailed explanation regarding Organizational Consultant's recommendation for the IOC's command and control process is given below.

> IOC should use meetings as means for coordination and control (cf 79). When IOC's environment has medium equivocality, high uncertainty, and high complexity, coordination and control should be obtained through integrators and group meetings. The richness of the media used should be medium with a large amount of information to cope with the environmental complexity and uncertainty. Incentives must be results based. Coordination within each division is very important. Coordination between (among) divisions is usually relegated to top management, which is also concerned about strategic direction and allocation of funds between (among) the divisions. Technology efficiencies can be obtained by sharing technology, information and new developments across divisions. Liaison managers and technology committees are possible coordination mechanisms. Conferences among technical professionals can be very effective. When the organization has a developmental climate, coordination should be obtained using planning, integrators and meetings. Incentives could be results based with an individual orientation. An

organization with a developmental climate will likely have to process a large amount of information and will need information media with high richness. [ORGCON, 1998]

3. More Detailed Recommendations

Organizational Consultant gave four detailed recommendations to further increase organizational effectiveness. These recommendations are all related to the level of formalization within the proposed Information Operations Council. The culmination of all of these recommendations leads the authors to conclude that by reducing the level of formalization within the IOC then there will be "good" organizational/design parameter fit. The four recommendations are listed below.

- Consider fewer written job descriptions.
- Managerial employees may be asked to pay less attention to written instructions and procedures.
- Consider having fewer rules and procedures put in writing.
- Consider decreasing the number of positions for which job descriptions are available.

F. CONCLUSION

The proposed Information Operations Council, after being analyzed through Organizational Consultant, will require further structural changes in order achieve a situation in which there are no misfits and all factors are consistent with one another. The situational misfits occur when there are inconsistencies between the organization's contingency factors (e.g. management style, size, environment, strategy). Although the

ideal organizational situation would be zero misfits, organizations can still be quite successful in meeting goals while certain misfits are present.

The situational misfits could be attributed to the fact that the proposed IOC is not a very typical organization. The IOC is an attempt to bring together a number of vastly diverse organizations with many different strategies and goals. The organization shows promise and can work with a few minor adjustments that will address the situational misfits.

The authors are satisfied with the results of the organization/design parameter misfits. There were only four misfits in this classification and all were related to there being too much formalization in the IOC. As stated previously, this type of misfit would be expected in most governmental organizations. This is not to say that because it is common it is acceptable, especially if a high degree of organizational formalization hinders performance. Excessive formalization frequently will suffocate the organization and promote complacency throughout. This point has been thoroughly discussed in previous sections of this chapter.

Lastly, the authors believe that two of the keys to successful implementation and operation of the Information Operations Council will be effective and efficient coordination, communication, and cohesion throughout the council; and the appropriate organizational configuration.

Efficient and effective coordination and communication will lead to cohesion between council members. What must be avoided, at all costs, is the thinking that each Departmental CIO works strictly for his or her specific department. There must be a

realization that the Departmental CIO's also work for the National CIO and within the council.

The authors have determined that the best organizational configuration would be the previously discussed "hybrid" configuration, which would combine aspects from both the divisional and matrix configurations. The Information Operations environment is one of great uncertainty and ambiguity. The traditional ways of organizing and strategizing may not be sufficient to handle this type of environment. Robert V. Hatcher, the chairman and CEO of Johnson and Higgins, states it best in an advertisement in the *Wall Street Journal:* "Either you take charge of change or change takes charge of you!"

VIII. FUTURE CONSIDERATIONS AND CONCLUSION

> The more epistemological the challenge, the more it may be confounding from an organizational standpoint. Whose responsibility is it to respond? Whose roles and missions are at stake? Is it a military, police, intelligence, or political matter? The roles and missions of defenders are not easy to define, and this may make both deterrence and defense quite problematic. [Arquilla and Ronfeldt, 1997, p.284]

A. FUTURE CONSIDERATIONS

In completing the circle that surrounds this thesis, it is important to note that in order to address the problem set forth, it had to be bounded. The area of focus was placed upon the organization at an executive inter-agency level. Many more deficiencies exist at different levels; it depends upon what boundaries are assigned and what type of environment is chosen.

The authors decided to analyze the proposed organization from a macro view and focused on only the upper management of the Information Operations Council. Additional value may be added by conceptually analyzing the IOC "from top to bottom" using Organizational Consultant. It may also be useful to analyze the organization using a program such as VITE, which focuses more on the individual actors, their inter-relations, and their tasks.

Law enforcement is based upon jurisdiction, whether their coverage is federal as in the FBI or local as in the State Police. Information knows no boundaries and therefore jurisdiction becomes a valid issue. Research into an IO Law Enforcement Agency would

be an important endeavor especially in the field of Intelligent Agents. A well-developed IO law enforcement agency would be a legitimate addition to the IOC, as it would need to address "information" type laws that are currently in the debate stages of government.

B. CONCLUSION

In the wake of the Information Revolution, the numerous means of information exchange have exposed weaknesses that have been the source of much attention; security, continuity, integrity and reliability. Although there are various methods and schools of thought to which information operations may be conducted, there must exist a cohesive policy and common structure from which those methods are employed. Policies, strategies and tactics all originate from an organization. Unfortunately if an organization is stagnant, "old school" and unwavering in its' approaches to new problems, then it is fair to say that policies and therefore the methods in which we approach information operations will too be considered...obsolete.

Global security has taken on a whole new meaning in the past ten years. Situations that seemed quite stable in the past have now become some of the focal points of instability. The lines between domestic and foreign policy, intelligence and information, political and economic agendas, as well as military and law enforcement activities are becoming increasingly blurred. The challenges of the future will be ambiguous and adversaries will have no respect for the traditional boundaries of the past. These vague lines must be constantly and thoroughly analyzed, evaluated, and updated to promote inter-agency coordination and efficiency. [NDP, 1997] It is important to state that the

changes suggested in this thesis are not a "one-time deal," these changes and suggestions must be constantly evaluated, and adjustments will have to be made in order to meet the requirements of a dynamic environment.

The purpose of this thesis has been to analyze the current Inter-Agency Information Operations organization, or lack there of. The authors have observed the deficiencies and inadequacies that are inherent within the current "system." The authors then developed and recommended a proposed Information Operations organization that would meet future United States National Security requirements; or more appropriately named the United States "National Information Operations Security."

The proposed solution is the establishment an inter-agency organization that would be titled the Information Operations Council (IOC). Its' primary goal would be to ensure that all relevant departments and agencies play their appropriate role in the formulation and implementation of both foreign and domestic Information Operations policy. The basis for this proposal is the current lack of integration between the various departments and agencies. The authors view the present Chief Information Officer Council, although having potential, as a victim of politics, bureaucracy, and "old school" thinking. The CIOC lacks the power and responsibility to address the problems that the USG faces today and in the future. Additionally the CIOC lacks any organizational, doctrinal, or strategic innovation, which inhibits the organization from adapting to meet new IO threats.

The current IO organizational structure is insufficient. It is a culmination of "individuals" from twenty-eight executive agencies that meet to develop

recommendations for information technology management issues, procedures, and standards; purely technologically driven. The majority of these individuals have taken on the position of departmental Information Officers not as their primary job, but as a collateral tasking. Unfortunately, in today's uncertain world, identifying the adversary/threat is becoming more and more difficult. Information Operations can no longer be thought of as a "part-time" job.

A National Chief Information Officer (NCIO) would head the proposed council. The NCIO would be directly appointed by the President and retain a seat on the National Security Council. This individual must be a fully qualified expert in the IO field. It is of the utmost importance that this position is not filled with a "figurehead," who is given the job through some type of political favor. The reason for appointing an official at this high level is because the USG needs a fully integrated inter-agency Information Operations Council that possesses the ability to incorporate IO policy and doctrine into National Security. The empowering of the NCIO would ensure that not only recommendations are made; but that IO policy is implemented across agency boundaries and that potential problems are addressed in an efficient and effective manner.

The government of the United States cannot assume that the simple infusion of new technologies and information systems into the previously successful doctrines, strategies, and organizational structures will guarantee dominance in the future information operations environment. Change and adaptation in "the way business is done" must be coupled with these innovations in technology. The United States may then

reach its' full IO potential and maintain informational dominance in the environment that will undoubtedly shape the future.

Gareth Morgan, "hits the nail on the head" in his book Riding the Waves of Change, by stating that organizations will either have to adapt to change or basically be overcome by change. Morgan states:

> Managers and their organizations are confronting wave upon wave of change in the form of new technologies, markets, forms of competition, social relations, forms of organization and management, ideas, beliefs, and so on. Wherever one looks, one sees a new wave coming. And it is vitally important that managers accept this as a fundamental aspect of their reality, rise to the challenge, and learn to ride or moderate these waves with accomplishment. This will require an approach to management and managerial competence that are proactive and future-oriented, so that future challenges will be talked with foresight and flexibility, and managers and their organizations will be able to deal with the opportunities created by the change, rather than allowing the waves to sweep them over. [Morgan, 1988, p.xii]

This statement holds true for any type of organization, whether it be commercial, military, or governmental. Change is a fundamental aspect of growth and expansion that must constantly be planned for and analyzed. This is the challenge that the Information Operations Council and all institutions within the United States government must answer to in the future.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. INPUTS TO ORGANIZATIONAL CONSULTANT

(ORGCON inputs are in **bold.**)

Current Configuration

1. What is the organization's current organizational configuration?
No answer
Simple
Functional
Divisional
Machine Bureaucracy
Professional Bureaucracy
Adhocracy
Matrix
Other
Certainty Factor: 75
The matrix configuration best suits this organization because it promotes interdepartmental cohesion and effective information distribution, which is the goal of the Information Operations Council. The organization will also possess some attributes from the divisional and machine bureaucracy configurations.

Current Complexity

1. How many different job titles are there?
No answer
Very few
Small number
Moderate number
Large number
Great number
Certainty Factor: 80
The analysis of this organization is from upper-middle management and higher so the number of different job titles will be moderate. If the organization was be analyzed from top to bottom, to include supporting staff then there would be a large number of different job titles.

2. What proportion of employees hold advanced degrees or have many years of specialized training?
No answer

0-10%
11-20%
21-50%
51-75%
76-100%
Certainty Factor: 85
All Departmental Chief Information officers will hold some type of relevant, advanced degree.

3. How many vertical levels separate the chief executive from those employees working at the bottom of the organization?
No answer
1 or 2
3 to 5
6 to 8
9 to 12
more than 12
Certainty Factor: 70
In this organizational structure the Chief Information Officer will have a CIO within each department/agency. Those departmental CIOs will each have their own IO support staff.

4. What is the average number of vertical levels for the organization?
No answer
1 or 2
3 to 5
6 to 8
9 to 12
more than 12
Certainty Factor: 70
See previous question.

5. Including the main center, how many geographic locations are there where organization members are employed?
No answer
1 or 2
3 to 5
6 to 15
16 to 30
more than 30
Certainty Factor: 70
All members of the council will be located in the main center—Washington, D.C.

6. What is the average distance of these outlying units from the organization's main center?
No answer
Less than 10 miles
11 to 100 miles
101 to 500 miles
501 to 3500 miles
more than 3500 miles
one site
Certainty Factor: 70
See previous question.

7. What proportion of the organization's total work force are located at these separate units?
No answer
Less than 10%
11 to 25%
26 to 60%
61 to 90%
more than 90%
one site
Certainty Factor: 75
Although support staffs will be widely dispersed, the main actors will be located in the main center.

Current Formalization

1. Written job descriptions available for?
No answer
none
operating employees or top management
operating employees and first line supervisors
operating employees, lower and middle management
all employees, excluding senior management
all employees, including senior management
Certainty Factor: 40
All members of the IO Council will have written job descriptions.

2. Where written job descriptions exist, how closely are employees supervised to ensure compliance with standards set in the job description?
No answer

very loose
loose
moderately close
close
very close
Certainty Factor: 80
Any type of governmental organization will ensure compliance with standards, but as stated earlier, the senior leadership must be given some latitude in decision making so as to allow them to "think outside of the box."

3. How much latitude are employees allowed from standards?
No answer
a great deal
large amount
a moderate amount
very little
none
Certainty Factor: 60
See previous question.

4. What percentage of non-managerial employees are given written operating instructions or procedures for their job?
No answer
0 to 20%
21 to 40%
41 to 60%
61 to 80%
more than 80%
Certainty Factor: 80
Standard Operating Procedures and written instruction are the norm in any governmental organization.

5. Of those managerial employees given written instructions or procedures, to what extent are they followed?
No answer
none
little
some
great deal
very great deal
no written instructions
Certainty Factor: 80

Orders should always be followed.

6. To what extent are supervisors and middle managers free from rules, procedures, and policies when they make decisions?
No answer
very great deal
great deal
some
little
none
Certainty Factor: 70
Again, for the majority of the time the operational activities will be dictated by standard operating procedures. But if the organization is going to be successful, it must give its managers the leeway to deviate from SOPs when the situation merits.

7. What percentage of all the rules and procedures that exist within the organization is in writing?
No answer
0 to 20%
21 to 40%
41 to 60%
61 to 80%
more than 80%
Certainty Factor: 80
The majority of all existing rules and procedures will be in writing.

Current Centralization

1. How much direct involvement does top management have in gathering the information they will use in making decisions?
No answer
none
little
some
great deal
very great deal
Certainty Factor: 70
Top management will be involved in the information gathering process to the extent of advising their subordinates what information they will need to assist in their decision

making process. The overall collection of information will be accomplished at the lower levels.

2. To what degree does top management participate in the interpretation of the information input?
No answer
0 to 20%
21 to 40%
41 to 60%
61 to 80%
more than 80%
Certainty Factor: 70
See previous question.

3. To what degree does top management directly control execution of a decision?
No answer
0 to 20%
21 to 40%
41 to 60%
61 to 80%
more than 80%
Certainty Factor: 80
Top management will be heavily involved in decision making process and in enforcing the execution of those decisions.

4. How much discretion does the typical middle manager have over establishing his or her budget?
No answer
very great
great
some
little
none
Certainty Factor: 80
Budget is determined outside of the organization.

5. How much discretion does the typical middle manager have over determining how his or her unit will be evaluated?
No answer
very great
great

some
little
none
Certainty Factor: 80
Not applicable.

6. How much discretion does the typical middle manager have over hiring and firing personnel?
No answer
very great
great
some
little
none
Certainty Factor: 80
Not applicable.

7. How much discretion does the typical middle manager have over personnel rewards (i.e. salary increases and promotions)?
No answer
very great
great
some
little
none
Certainty Factor: 80
Not applicable.

8. How much discretion does the typical middle manager have over purchasing equipment and supplies?
No answer
very great
great
some
little
none
Certainty Factor: 80
Not applicable.

9. How much discretion does the typical middle manager have over establishing a new project or program?
No answer

very great
great
some
little
none
Certainty Factor: 70
The "out of the box" thinking will promote innovation, which in turn will encourage middle managers to voice their opinions and ideas.

10. How much discretion does the typical middle manager have over how work exceptions are to be handled?
No answer
very great
great
some
little
none
Certainty Factor: 70
There will be some management of work exceptions, but for the most part work exceptions will be few and far between since most of the rules and procedures are in writing.

Size

1. How many employees does this organization have?
Input any number: 200
Certainty Factor: 50
Although the total organization will have well over 2,000 employees, the authors are only analyzing the organization from middle management and higher.

Age/Ownership

1. How old is the organization?
No answer
young
mature
old
Certainty Factor: 90
This organization is still in the conceptual/development phase.

2. What kind of ownership does the organization have?
No answer
private
incorporated
public/state owned
subsidiary
Certainty Factor: 100

Diversity

1. Does the organization have many different products?
No answer
many
some
few
Certainty Factor: 80
There are many different informational products that will be produced by the IOC.

2. Does the organization operate in many different markets?
No answer
many
some
few
Certainty Factor: 80
The IOC will operate throughout the world.

3. Does the organization operate in more than one country? If yes, is the activity level abroad greater than 25%?
No answer
Yes - activity level greater than 25%
Yes - activity level lower than 25% no
Certainty Factor: 60
There is basically 50% of the organization's assets devoted to the international environment and 50% to the domestic environment.

4. Does the organization have many different products in the foreign market?
No answer
many
some

few
none
Certainty Factor: 70

Technology

1. What is the major activity of the organization?
No answer
production
service
retail
wholesale
Certainty Factor: 60
The IOC safeguards the informational infrastructure of the U.S.

2. What kind of technology does the organization have?
No answer
standard high volume retail
high automated retail
specialized customer oriented retail
Certainty Factor: 80
The organization is not involved in any type of retail.

3. Does the organization have a routine technology?
No answer
no
some
yes
Certainty Factor: 60

4. Is the technology divisible?
No answer
highly
somewhat
little
Certainty Factor: 70
Some of the everyday jobs can be further broken down in to smaller tasks, while others cannot be broken down.

5. Does the organization have a strong or weak dominant technology?
No answer
weak
average
strong
Certainty Factor: 80
The organization will be very reliant upon strong information processing systems, communication systems, and decision support systems.

6. Does the organization use or plan to use an advanced information system?
No answer
yes
no
Certainty Factor: 100
Advanced information systems will play a key role in successful information operations.

Environment

1. Is the organizational environment simple or complex?
No answer
simple
some
complex
Certainty Factor: 100
The information operations environment is purely complex.

2. What is the level of uncertainty of the environment?
No answer
low
medium
high
Certainty Factor: 90
The IO environment is in constant flu and uncertainty.

3. Is the equivocality of the environment low or high?
No answer
low
medium
high

Certainty Factor: 80
The environment is somewhat ambiguous.

4. Is the organizational environment hostile - how tough is the competition?
No answer
extreme
high
medium
low
Certainty Factor: 80
The organization's competition/threats are highly competitive very hostile.

Management Profile

1. Top management may prefer to make most of the decisions themselves; or they may prefer to delegate numerous decisions to other managers i.e.;, greater preference for decentralization. What kind of decisions does top management prefer to make?
No answer
policy and general decisions
both general and some operating decisions
both general and operating decisions
Certainty Factor: 70
The National Chief Information Officer will make the majority of the policy and general decisions through the inputs he receives from the departmental Information Officers.

2. Top management may prefer to make long-term decision or short-time decision. What kind of decisions does top management prefer to make?
No answer
long term
long term and short time
short time
Certainty Factor: 80
The National Chief Information Officer will have a large influence on both long and short-term decisions and policy.

3. Top management may prefer to use very detailed or very aggregate information when making decisions. What level of detail of information does top management prefer to use when making decisions?
No answer
very detailed information
medium detailed information
very aggregate information
Certainty Factor: 70
Top management will require some detailed information in order to make educated decisions.

4. Top management may prefer to be proactive in its thinking, anticipate future events and take pre-emptive action. It may be reactive; wait and see and then act. What is management's preference on taking action?
No answer
proactive anticipating future events
some proactive and some reactive
reactive to events as they occur
Certainty Factor: 90
Being proactive and anticipating future events will be an essential factor in organizational success.

5. Top management may be risk averse in its decision-making or it may have a preference to assume risk. What is top management's attitude towards risk?
No answer
risk propensity
risk neutral
risk adverse
Certainty Factor: 75
There will be certain situations where top management will need to be risk adverse and other situations where a certain level of risk will be expected.

6. Top management may prefer to manage through an ex ante motivation or ex post control techniques. What kind of motivation and control does top management prefer?
No answer
motivation through inspiration
a combination of motivation and control using control techniques
Certainty Factor: 60

Strategy Factors

1. Does the organization have a high or low capital requirement?
No answer
high
medium
low
Certainty Factor: 60
Almost all Information Operations have a large capital requirement.

2. Does the organization have high or low product innovation?
No answer
high
medium
low
Certainty Factor: 70
Innovation is another key factor in organizational success.

3. Does the organization have high or low process innovation?
No answer
high
medium
low
Certainty Factor: 70
Process innovation is required in order for the organization to adapt to the constant changes in the operational environment.

4. Does the organization have a high or low concern for quality?
No answer
high
medium
low
Certainty Factor: 80
Quality of information is another key to organizational success.

5. How is the organization's price level compared to its competitors?
No answer
high
medium
low

Certainty Factor: 100
Not applicable.

Climate Factors

1. The level of trust - sharing, openness, trust - is:
No answer
high
medium
low
Certainty Factor: 80
Trust within the organization will be high, but outside the organization the trust level will be significantly lower.

2. The level of conflict - disagreement, friction - in this organization is:
No answer
high
medium
low
Certainty Factor: 80

3. The employee morale - confidence, enthusiasm - in this organization is:
No answer
high
medium
low
Certainty Factor: 70

4. Rewards are given in an equitable fashion:
No answer
highly equitable
moderately equitable
inequitable
Certainty factor: 80
Not applicable.

5. The organization's resistance to change is:
No answer
high

medium
low
Certainty Factor: 75
Although most government organizations are highly resistant to change and are extremely bureaucratic in nature, the Information Operations Council must be open to change and adaptation.

6. The leadership credibility - respect, inspiration, acceptance - is:
No answer
high
medium
low
Certainty Factor: 90
As with any organization, the acceptance and credibility of its leaders must be high if the organization will be successful.

7. The level of scapegoating - shifting of responsibility for actions which fail - is:
No answer
high
medium
low
Certainty Factor: 70

APPENDIX B. ORGCON RESULTS

REPORT SUMMARY - IOC

Time: 2:13:19 PM, 3/13/2001
Scenario: Basic

INPUT DATA SUMMARY

The description below summarizes and interprets your answers to the questions about your organization and its situation. It states your answers concerning the organization's current configuration, complexity, formalization, and centralization. Your responses to the various questions on the contingencies of age, size, technology, environment, management style, cultural climate and strategy factors are also given. The write-up below summarizes the input data for the analysis.

- IOC has a divisional configuration (cf 75).
- IOC has a moderate number of different jobs (cf 80).
- Of the employees at IOC 76 to 100 % have an advanced degree or many years of special training (cf 85).
- IOC has 3 to 5 vertical levels separating top management from the bottom level of the organization (cf 70).
- The mean number of vertical levels is 3 to 5 (cf 70).
- IOC has 1 or 2 separate geographic locations (cf 80).
- IOC's average distance of these separate units from the organization's headquarters is less than 10 miles (cf 70).
- 11 to 25 % of IOC's total workforce is located at these separate units (cf 75).
- Job descriptions are available for all employees, including senior management (cf 40).
- Where written job descriptions exist, the employees are supervised moderately closely to ensure compliance with standards set in the job description (cf 80).
- The employees are allowed to deviate a moderate amount from the standards (cf 60).
- 61 to 80 % non-managerial employees are given written operating instructions or procedures for their job (cf 80).
- The written instructions or procedures given are followed to a great extent (cf 80).
- Supervisors and middle managers are to some extent free from rules, procedures, and policies when they make decisions (cf 70).
- 61 to 80 % of all the rules and procedures that exist within the organization are in writing (cf 80).
- Top Management is only a little involved in gathering the information they will use in making decisions (cf 70).
- Top management participates in the interpretation of 21 to 40 % of the information input (cf 70).

- Top management directly controls 61 to 80 % of the decisions executed (cf 80).
- The typical middle manager has an undetermined amount of discretion over establishing his or her budget (cf 100).
- The typical middle manager has an undetermined discretion over how his/her unit will be evaluated (cf 100).
- The typical middle manager has an undetermined amount of discretion over the hiring and firing of personnel (cf 100).
- The typical middle manager has an undetermined discretion over personnel rewards - (i.e., salary increases and promotions) (cf 100).
- The typical middle manager has an undetermined discretion over purchasing equipment and supplies (cf 100).
- The typical middle manager has some discretion over establishing a new project or program (cf 70).
- The typical middle manager has some discretion over how work exceptions are to be handled (cf 70).
- IOC has 200 employees (cf 80).
- IOC's age is young (cf 90).
- IOC's ownership status is public (cf 100).
- IOC has many different products (cf 80).
- IOC has many different markets (cf 80).
- IOC operates at a high-activity level in more countries (cf 60).
- IOC has many different products in the foreign markets (cf 70).
- IOC's major activity is categorized as service (cf 60).
- IOC has an undetermined service technology (cf 100).
- IOC has a medium routine technology (cf 60).
- IOC's technology is somewhat divisible (cf 70).
- IOC's technology dominance is strong (cf 80).
- IOC has either planned or already has an advanced information system (cf 100).
- IOC's environment is complex (cf 100).
- The uncertainty of IOC's environment is high (cf 90).
- The equivocality of the organization's environment is medium (cf 80).
- IOC's environment has a high hostility (cf 80).
- Top management prefers to make policy and general resource allocation decisions (cf 70).
- Top management primarily prefers to make both long-term and short-time decisions (cf 80).
- Top management has a preference for medium detailed information when making decisions (cf 70).
- Top management has a preference for proactive actions (cf 90).
- Top management is risk neutral (cf 75).
- Top management has a preference for a combination of motivation and control (cf 60).
- IOC operates in an industry with a high capital requirement (cf 60).
- IOC has a high product innovation (cf 70).

- IOC has a high process innovation (cf 70).
- IOC has a high concern for quality (cf 80).
- IOC's price level is undetermined relative to its competitors (cf 100).
- The level of trust is medium (cf 80).
- The level of conflict is medium (cf 80).
- The employee morale is high (cf 70).
- Rewards are given in a not known fashion (cf 100).
- The resistance to change is medium (cf 75).
- The leader credibility is high (cf 90).
- The level of scapegoating is medium (cf 70).

THE SIZE

The size of the organization - large, medium, or small - is based upon the number of employees, adjusted for their level of education or technical skills.

Based on the answers you provided, it is most likely that your organization's size is medium (cf 80).

More than 75 % of the people employed by IOC have a high level of education. Adjustments are made to this effect. The adjusted number of employees is lower than 1,000 but greater than 500 and IOC is categorized as having a medium size.

THE CLIMATE

The organizational climate effect is the summary measure of people and behavior.

Based on the answers you provided, it is most likely that the organizational climate is a developmental climate (cf 64).

The developmental climate is characterized as a dynamic, entrepreneurial and creative place to work. People stick their necks out and take risks. The leaders are considered to be innovators and risk takers. The glue that holds organizations together is commitment to experimentation and innovation. The emphasis is on being on the leading edge. Readiness for change and meeting new challenges are important. The organization's long-term emphasis is on growth and acquiring new resources. Success means having unique and new products or services and being a product or service leader is important. The organization encourages individual initiative and freedom.

Medium to high leader credibility characterizes an organization with a developmental climate. When the organization has a high to medium level of trust it is likely that the organization has a developmental climate. Employees with a high morale is frequently

one element of a developmental climate. An organization with a medium level of scapegoating may have a developmental climate.

THE MANAGEMENT STYLE

The level of management's micro-involvement in decision-making is the summary measure of management style. Leaders have a low preference for micro-involvement; managers have a high preference for micro-involvement.

Based on the answers you provided, it is most likely that your management profile has a medium preference for micro-involvement (cf 73).

Management has both a short-time and long-term horizon when making decisions, which characterizes a preference for a medium micro-involvement. Management is risk neutral. This is one of the characteristics of a manager with a medium preference for micro-involvement. Since the management has a preference for medium detailed information when making decisions a medium preference for micro-involvement characterization is appropriate. Management has a preference for using both motivation and control to coordinate the activities, which leads toward a medium preference for micro-involvement.

THE STRATEGY

The organization's strategy is categorized as one of either prospector, analyzer with innovation, analyzer without innovation, defender, or reactor. These categories follow Miles and Snow's typology. Based on your answers, the organization has been assigned to a strategy category. This is a statement of the current strategy; it is not an analysis of what is the best or preferred strategy for the organization.

Based on the answers you provided, it is most likely that your organization's strategy is an analyzer with innovation strategy (cf 68).

It could also be: a prospector (cf 65).

An organization with an analyzer with innovation strategy is an organization that combines the strategy of the defender and the prospector. It moves into the production of a new product or enters a new market after viability has been shown. But in contrast to an analyzer without innovation, it has innovations that run concurrently with the regular production. It has a dual technology core.
With a concern for high quality an analyzer with innovation strategy is a likely strategy for IOC. With top management preferring a medium level of micro-involvement top

management wants some influence. This can be obtained via control over current operations. Product innovation should be less controlled. The strategy is therefore likely to be analyzer with innovation. For a medium routine technology, IOC has some flexibility. It is consistent with an analyzer with innovation strategy.

An organization with a prospector strategy is an organization that continually searches for market opportunities and regularly experiments with potential responses to emerging environmental trends. Thus, the organization is often the creator of change and uncertainty to which its competitors must respond. However, because of its strong concern for product and market innovation, a prospector usually is not completely efficient.
IOC has numerous products. A prospector is constantly seeking new product opportunities to serve the existing and potentially new customers. With a concern for high quality a prospector strategy is a likely strategy for IOC. For a prospector strategy to be aggressive in product development or market opportunities exploitation, it requires a high capital investment.

THE CURRENT ORGANIZATIONAL CHARACTERISTICS

Based on your answers, the organization's complexity, formalization, and centralization have been calculated. This is the current organization. Later in this report, there will be recommendations for the organization.

The current organizational complexity is medium (cf 75).

The current horizontal differentiation is high (cf 80).

The current vertical differentiation is low (cf 70).

The current spatial differentiation is low (cf 70).

The current centralization is medium (cf 86).

The current formalization is high (cf 70).

The current organization has been categorized with respect to formalization, centralization, and complexity. The categorization is based on the input you gave and does not take missing information into account.

SITUATION MISFITS

A situation misfit is an unbalanced situation among the contingency factors of management style, size, environment, technology, climate, and strategy.

The following misfits are present: (cf 100).

IOC has a high capital requirement but is not a large organization. The organization can be vulnerable. An organization with a high capital requirement and a few employees usually makes a few standardized products. Further, the technology is likely to be very limited in adaptiveness. The organization is then vulnerable to changes in the environment, market and products changes. Smaller organizations with small capital requirements are frequently more adaptive. To reduce this vulnerability, the organization should consider creating a greater capability for adaptation, which will usually require more employees of higher skill, education and training.

ORGANIZATIONAL CONSULTANT RECOMMENDATIONS

Based on your answers about the organization, its situation, and the conclusions with the greatest certainty factor from the analyses above Organizational Consultant has derived recommendations for the organization's configuration, complexity, formalization, and centralization. There are also recommendations for coordination and control, the appropriate media richness for communications, and incentives. More detailed recommendations for possible changes in the current organization are also provided.

ORGANIZATIONAL CONFIGURATIONS

The most likely configuration that best fits the situation has been estimated to be a divisional configuration (cf 69).

It is certainly not: a machine bureaucracy (cf -80).

A divisional organization is an organization with self-contained unit grouping into relatively autonomous units coordinated by a headquarters, (product, customer, or geographical grouping).
When the organization is of medium size, the configuration can be a divisional configuration. Because the organization has many products, the configuration should be

divisional. The configuration should be divisional when the equivocality of IOC's environment is not high and the complexity is not low. The divisionalization of IOC may be based on products or product groups. The divisionalization of IOC may be based on markets. The divisional configuration may be a multi-domestic structure.
Because the technology is not fully divisible, care should be taken in recommending a divisional configuration.
When the organization has high hostility, it is unlikely to be a machine bureaucracy. A machine bureaucracy will prevent it from acting appropriately when unexpected events occur.

ORGANIZATIONAL CHARACTERISTICS

The recommended degree of organizational complexity is medium (cf 62).

Medium size organizations should have medium organizational complexity. IOC has a technology that is somewhat routine, which implies that the organizational complexity should be medium. The environmental uncertainty of IOC is high, and the equivocality of IOC's environment is medium. For this situation the organizational complexity should be medium. There is no need for an elaborate hierarchy or work specialization. Top management of IOC has a preference for a medium level of micro-involvement, which drives the organizational complexity towards medium. Because IOC has an advanced information system, organizational complexity can be greater than it could otherwise. A developmental climate in the organization requires a medium level of complexity.

The recommended degree of horizontal differentiation is medium (cf 27).

The recommended degree of vertical differentiation is medium (cf 48).

It, too, could be: low (cf 44).

The recommended degree of formalization is medium (cf 53).

There should be some formalization between the organizational units but less formalization within the units due to the high professionalization. Medium size organizations should have medium formalization. Organizations with medium-routine technology should have a medium formalization. Medium formalization is consistent with the leadership style when top management's preference for micro-involvement is neither very great nor very low.

The recommended degree of centralization is medium (cf 59).

IOC has an analyzer with innovation strategy. Centralization should be medium. There should be tight control over current activities and looser control over new ventures. When there is a high capital requirement and the product innovation is high, as is the case for IOC, centralization should be medium. IOC is of medium size. Such organizations should have medium to high centralization. Medium centralization is recommended when top management has neither a great desire nor very little desire for micro-involvement. Because IOC has an advanced information system, centralization can be greater than it could otherwise. A developmental climate in the organization requires a medium to low level of centralization.

IOC's span of control should be moderate (cf 49).

Since IOC has some technology routineness, it should have a moderate span of control.

IOC should use media with medium media richness (cf 70).

The information media that IOC uses should provide a large amount of information (cf 85).

Incentives should be based on results (cf 85).

IOC should use meetings as means for coordination and control (cf 79).

When IOC's environment has medium equivocality, high uncertainty, and high complexity, coordination and control should be obtained through integrators and group meetings. The richness of the media used should be medium with a large amount of information to cope with the environmental complexity and uncertainty. Incentives must be results based. Coordination within each division is very important. Coordination between (among) divisions is usually relegated to top management, which is also concerned about strategic direction and allocation of funds between (among) the divisions. Technology efficiencies can be obtained by sharing technology, information and new developments across divisions. Liaison managers and technology committees are possible coordination mechanisms. Conferences among technical professionals can be very effective. When the organization has a developmental climate, coordination should be obtained using planning, integrators and meetings. Incentives could be results based with an individual orientation. An organization with a developmental climate will likely have to process a large amount of information and will need information media with high richness.

ORGANIZATIONAL MISFITS

Organizational misfits compares the recommended organization with the current organization.

The following organizational misfits are present: (cf 100).

Current and prescribed formalization do not match.

MORE DETAILED RECOMMENDATIONS

There are a number of more detailed recommendations (cf 100).

You may consider fewer written job descriptions.
Managerial employees may be asked to pay less attention to written instructions and procedures.
You may consider having fewer rules and procedures put in writing.
You may consider decreasing the number of positions for which job descriptions are available.

END

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. LIST OF ACRONYMS

AAG/A	-	Assistant Attorney General for Administration
ACDA	-	Arms Control and Disarmament Agency
ADR	-	Alternate Dispute Resolution
AG	-	Attorney General
ASD	-	Assistant Secretary of Defense
ATF	-	Bureau of Alcohol, Tobacco & Firearms
BEP	-	Bureau of Engraving and Printing
BLS	-	Bureau of Labor Statistics
BOP	-	Bureau of Prisons
BPD	-	Bureau of the Public Debt
BPI	-	Business Process Improvement
BTS	-	the Bureau of Transportation Statistics
BXA	-	Bureau of Export Administration
C3I	-	Command, Control, Communications and Intelligence
C3ISR	-	C3I, Surveillance and Reconnaissance
CA	-	Civil Affairs
CDC	-	Center for Disease Control and Prevention
CDFI	-	Community Development Financial Institutions
cf	-	Certainty Factor
CFO	-	Chief Financial Officer
CIA	-	Central Intelligence Agency
CIO	-	Chief Information Officer
CNA	-	Computer Network Attack
CND	-	Computer Network Defense
CPO	-	Chief Procurement Officer
CSM	-	Committee of Special Means
DASD	-	Deputy Assistant Secretary of Defense

DASIRM	-	Deputy Assistant Secretary of Information Resources Management
DCI	-	Director of Central Intelligence
DDCI	-	Deputy Director of Central Intelligence
DDOS	-	Distributed Denial of Service
DEA	-	Drug Enforcement Administration
DIO	-	Departmental Information Officer
DOC	-	Department of Commerce
DOD	-	Department of Defense
DOE	-	Department of Energy
DOEd	-	Department of Education
DHUD	-	Department of Housing and Urban Development
DOI	-	Department of the Interior
DOINET	-	Department of the Interior Network
DOJ	-	Department of Justice
DOL	-	Department of Labor
DON	-	Department of the Navy
DOS	-	Department of State
DOT	-	Department of Transportation
DWC	-	Department Webmaster's Council
EA	-	Enterprise Architecture
EDA	-	Economic Development Administration
EPA	-	Environmental Protection Agency
ESA	-	Economics and Statistics Administration
		or Employment Standards Administration
ETA	-	Employment & Training Administration
EW	-	Electronic Warfare
EXDIR	-	Executive Director
FAA	-	Federal Aviation Administration
FBI	-	Federal Bureau of Investigation
FCC	-	Federal Communications Commission
FDA	-	Food and Drug Administration
FinCEN	-	Financial Crimes Enforcement Network

FLETC	-	Federal Law Enforcement Training Center
FMS	-	Financial Management Service
FRA	-	Federal Railroad Administration
FTA	-	Federal Transit Administration
FTC	-	Federal Trade Commission
FEMA	-	Federal Emergency Management Agency
FHWA	-	Federal Highway Administration
FMCSA	-	Federal Motor Carrier Safety Administration
GILS	-	Government Information Locator System
HHS	-	Department of Health & Human Services
HUD	-	Department of Housing and Urban Development
IA	-	Information Assurance
IC	-	Intelligence Community
IG	-	Inspector General
ILAB	-	Bureau of International Labor Affairs
INS	-	Immigration and Naturalization Service
IO	-	Information Operations
IRM	-	Information Resource Management
IRS	-	Internal Revenue Service
IS	-	Information Systems
ISSB	-	Inter-Services Security Board
IT	-	Information Technology
ITA	-	International Trade Administration
ITM	-	Information Technology Management
IW	-	Information Warfare
JCS	-	Joint Chiefs of Staff
JSC	-	Joint Security Control
JMD	-	Justice Management Division
LAN	-	Local Area Network

LCS	-	London Controlling Section
MARAD	-	Maritime Administration
MBDA	-	Minority Business Development Agency
MI(R)	-	Military Intelligence - Research
MSHA	-	Mine Safety and Health Administration
NHTSA	-	National Highway Traffic Safety Administration
NIC	-	National Intelligence Council
NTIA	-	National Telecommunications & Information Administration
NOAA	-	National Oceanic and Atmospheric Administration
NPS	-	Naval Postgraduate School
NSA	-	National Security Agency
NSC	-	National Security Council
OASAM	-	Office of the Assistant Secretary for Administration & Management
OASP	-	Office of the Assistant Secretary for Policy
OCC	-	Office of the Comptroller of the Currency
OCFO	-	Office of the Chief Financial Officer
OCS	-	Office of Computer Services
OEI	-	Office of Environmental Information
OIAA	-	Office of Information Analysis and Access
OIC	-	Office of Information Collection
OICA	-	Office of Information Collection and Analysis
OIG	-	Office of the Inspector General
OIPR	-	Office of Information Planning and Review
OIPT	-	Office of Information Policy and Technology
OIS	-	Office of Information Systems
OI&T	-	Office of Information & Technology
OKW	-	Oberkommando der Wehrmacht or High Command of the Armed Forces
OMB	-	Office of Management & Budget
OPA	-	Office of Public Affairs

OPDIV	-	Operating Division
OPSEC	-	Operational Security
OSBP	-	Office of Small Business Programs
OSD	-	Office of the Secretary of Defense
OSHA	-	Occupational Safety & Health Administration
OSS	-	Office of Strategic Services
OST	-	Office of the Secretary of Transportation
OTM	-	Office of Telecommunications Management
OTOP	-	Office of Technology, Operations and Planning
OTS	-	Office of Thrift Supervision
OTS&NS	-	Office of Technical Support and Network Services
PA	-	Public Affairs
PMB	-	Policy, Management & Budget
PTO	-	Patent and Trademark Office
PWBA	-	Pension & Welfare Benefits Administration
QA	-	Quality Assurance
RAF	-	Royal Air Force
RMP	-	Records Management Program
RSPA	-	Research and Special Programs Administration
SD	-	Sicherheitsdienst or Security Police
SEC	-	Securities and Exchange Commission
SIS	-	Secret Intelligence Service
SLSDC	-	Saint Lawrence Seaway Development Corporation
SOE	-	Special Operations Executive
SOL	-	Office of the Solicitor
SS	-	Schutzstaffel or Protective Squadrons
SSA	-	Social Security Administration
STB	-	Surface Transportation Board
TA	-	Technology Administration

TASC	-	Transportation Administrative Services Center
TFF	-	Treasury Forfeiture Fund
TIBEC	-	Technology Investment Board Executive Committee
TM	-	Technology Management
U.S.	-	Untied States
USA	-	United States Army
USAF	-	United States Air Force
USAID	-	United States Agency for International Development
USCG	-	United States Coast Guard
USDA	-	United States Department of Agriculture
USN	-	United States Navy
USMC	-	United States Marine Corps
USMS	-	United States Marshal Service
USSS	-	United States Customs Service
VA	-	Department of Veteran's Affairs
VBA	-	Veteran's Benefits Administration
VHA	-	Veteran's Health Administration
VETS	-	Veteran's Employment & Training Service
WB	-	Women's Bureau
WMD	-	Weapons of Mass Destruction
XX	-	Double Cross Committee

APPENDIX D. IO TERMINOLOGY & DEFINITIONS

Computer Network Attack – operations conducted to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.

Computer Network Defense – operations and precautions conducted to disrupt, deny or destroy an adversary's ability to attack information resident in your computers and computer networks or your computers and networks themselves.

Deception – measures designed to mislead an adversary by manipulation, distortion, or falsification of evidence to induce a reaction prejudicial to that adversary's interest.

Information - facts, data, or instructions in any medium or form. It is the meaning that a human assigns to data by means of the known conventions used in their representation. The same information may hold different levels of importance to different users.

Information Operations - actions taken to affect adversary information and information systems, while defending one's own information and infrastructure. IO may include, but is not limited to: Operational Security (OPSEC), Psychological Operations (PSYOP), Military Deception, Electronic Warfare (EW), attack/destruction via physical and/or computer means, Public Affairs (PA), and Civil Affairs (CA).

Information Assurance - information operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Superiority – the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information System – the entire infrastructure, organization, personnel, and components, that collect, process, store, transmit, display, disseminate, and act on information as well as the information-based processes.

Information Warfare – information operations conducted during time of crisis or conflict in order to promote specific objectives over a specific adversary.

National Information Infrastructure – the nation-wide interconnection of communication networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The infrastructure encompasses a wide range of equipment including cameras, scanners, keyboards, facsimile machines, computers, switches, routers, information storage devices, satellites, transmission lines, monitors, printers and much more.

Perception Management – actions taken to convey and/or deny selected information and indicators to a targeted audience in order to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in behaviors and official actions that are desirable.

Psychological Operations – operations planned to convey selected information and indicators to a targeted audience by influencing their emotions, motives, objective reasoning and ultimately their behavior. The purpose of these types of operations is to induce or reinforce attitudes and behavior that support an overall plan.

Public Affairs – those public information, organizational information, and community relations' activities directed toward both the external and internal publics.

Special Information Operations – information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the U.S., require a special review and overall process.

APPENDIX E. EXECUTIVE ORDER 13011 OF JULY 16, 1996

FEDERAL INFORMATION TECHNOLOGY

A Government that works better and costs less requires efficient and effective information systems. The Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 provide the opportunity to improve significantly the way the Federal Government acquires and manages information technology. Agencies now have the clear authority and responsibility to make measurable improvements in mission performance and service delivery to the public through the strategic application of information technology. A coordinated approach that builds on existing structures and successful practices is needed to provide maximum benefit across the Federal Government from this technology.

Accordingly, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. It shall be the policy of the United States Government that executive agencies shall:

(a) significantly improve the management of their information systems, including the acquisition of information technology, by implementing the relevant provisions of the Paperwork Reduction Act of 1995 (Public Law 104-13), the Information Technology Management Reform Act of 1996 (Division E of Public Law 104-106) ("Information Technology Act"), and the Government Performance and Results Act of 1993 (Public Law 103-62);

(b) refocus information technology management to support directly their strategic missions, implement an investment review process that drives budget formulation and execution for information systems, and rethink and restructure the way they perform their functions before investing in information technology to support that work;

(c) establish clear accountability for information resources management activities by creating agency Chief Information Officers (CIOs) with the visibility and management responsibilities necessary to advise the agency head on the design, development, and implementation of those information systems. These responsibilities include: (1) participating in the investment review process for information systems; (2) monitoring and evaluating the performance of those information systems on the basis of applicable performance measures; and, (3) as necessary, advising the agency head to modify or terminate those systems;

(d) cooperate in the use of information technology to improve the productivity of Federal programs and to promote a coordinated, interoperable, secure, and shared Government-wide infrastructure that is provided and supported by a diversity of private sector suppliers and a well-trained corps of information technology professionals; and

(e) establish an interagency support structure that builds on existing successful interagency efforts and shall provide expertise and advice to agencies; expand the skill and career development opportunities of information technology professionals; improve the management and use of information technology within and among agencies by developing information technology procedures and standards and by identifying and sharing experiences, ideas, and promising practices; and provide innovative, multi-disciplinary, project-specific support to agencies to enhance interoperability, minimize unnecessary duplication of effort, and capitalize on agency successes.

Sec. 2. Responsibilities of Agency Heads. The head of each executive agency shall:

(a) effectively use information technology to improve mission performance and service to the public;

(b) strengthen the quality of decisions about the employment of information resources to meet mission needs through integrated analysis, planning, budgeting, and evaluation processes, including:

(1) determining, before making investments in new information systems, whether the Government should be performing the function, if the private sector or another agency should support the function, and if the function needs to be or has been appropriately redesigned to improve its efficiency;

(2) establishing mission-based performance measures for information systems investments, aligned with agency performance plans prepared pursuant to the Government Performance and Results Act of 1993 (Public Law 103-62);

(3) establishing agency-wide and project-level management structures and processes responsible and accountable for managing, selecting, controlling, and evaluating investments in information systems, with authority for terminating information systems when appropriate;

(4) supporting appropriate training of personnel; and

(5) seeking the advice of, participating in, and supporting the interagency support structure set forth in this order;

(c) select CIOs with the experience and skills necessary to accomplish the duties set out in law and policy, including this order, and involve the CIO at the highest level of the agency in the processes and decisions set out in this section;

(d) ensure that the information security policies, procedures, and practices of the executive agency are adequate;

(e) where appropriate, and in accordance with the Federal Acquisition Regulation and guidance to be issued by the Office of Management and Budget (OMB), structure major information systems investments into manageable projects as narrow in scope and brief in duration as practicable, consistent with the Information Technology Act, to reduce risk, promote flexibility and interoperability, increase accountability, and better correlate mission need with current technology and market conditions; and

(f) to the extent permitted by law, enter into a contract that provides for multi-agency acquisitions of information technology as an executive agent for the Government, if and in the manner that the Director of OMB considers it advantageous to do so.

Sec. 3. Chief Information Officers Council. (a) **Purpose and Functions.** A Chief Information Officers Council ("CIO Council") is established as the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources. The Council shall:

(1) develop recommendations for overall Federal information technology management policy, procedures, and standards;

(2) share experiences, ideas, and promising practices, including work process redesign and the development of performance measures, to improve the management of information resources;

(3) identify opportunities, make recommendations for, and sponsor cooperation in using information resources;

(4) assess and address the hiring, training, classification, and professional development needs of the Federal Government with respect to information resources management;

(5) make recommendations and provided advice to appropriate executive agencies and organizations, including advice to OMB on the Government-wide strategic plan required by the Paperwork Reduction Act of 1995; and

(6) seek the views of the Chief Financial Officers Council, Government Information Technology Services Board, Information Technology Resources Board, Federal Procurement Council, industry, academia, and State and local governments on matters of concern to the Council as appropriate.

(b) **Membership.** The CIO Council shall be composed of the CIOs and Deputy CIOs of the following executive agencies plus two representatives from other agencies:

1. Department of State;

2. Department of the Treasury;
3. Department of Defense;
4. Department of Justice;
5. Department of the Interior;
6. Department of Agriculture;
7. Department of Commerce;
8. Department of Labor;
9. Department of Health and Human Services;
10. Department of Housing and Urban Development;
11. Department of Transportation;
12. Department of Energy;
13. Department of Education;
14. Department of Veterans Affairs;
15. Environmental Protection Agency;
16. Federal Emergency Management Agency;
17. Central Intelligence Agency;
18. Small Business Administration;
19. Social Security Administration;
20. Department of the Army;
21. Department of the Navy;
22. Department of the Air Force;
23. National Aeronautics and Space Administration;
24. Agency for International Development;
25. General Services Administration;
26. National Science Foundation;

27. Nuclear Regulatory Commission; and

28. Office of Personnel Management.

The Administrator of the Office of Information and Regulatory Affairs of OMB, the Controller of the Office of Federal Financial Management of OMB, the Administrator of the Office of Federal Procurement Policy of OMB, a Senior Representative of the Office of Science and Technology Policy, the Chair of the Government Information Technology Services Board, and the Chair of the Information Technology Resources Board shall also be members. The CIO Council shall be chaired by the Deputy Director for Management of OMB. The Vice Chair, elected by the CIO Council on a rotating basis, shall be an agency CIO.

Sec. 4. Government Information Technology Services Board.

(a) **Purpose and Functions.** A Government Information Technology Services Board ("Services Board") is established to ensure continued implementation of the information technology recommendations of the National Performance Review and to identify and promote the development of innovative technologies, standards, and practices among agencies and State and local governments and the private sector. It shall seek the views of experts from industry, academia, and State and local governments on matters of concern to the Services Board as appropriate. The Services Board shall also make recommendations to the agencies, the CIO Council, OMB, and others as appropriate, and assist in the following:

(1) creating opportunities for cross-agency cooperation and intergovernmental approaches in using information resources to support common operational areas and to develop and provide shared Government-wide infrastructure services;

(2) developing shared Government-wide information infrastructure services to be used for innovative, multi-agency information technology projects;

(3) creating and utilizing affinity groups for particular business or technology areas; and

(4) developing with the National Institute of Standards and Technology and with established standards bodies, standards and guidelines pertaining to Federal information systems, consistent with the limitations contained in the Computer Security Act of 1987 (40 U.S.C. 759 note), as amended by the Information Technology Act.

(b) **Membership.** The Services Board shall be composed of individuals from agencies based on their proven expertise or accomplishments in fields necessary to achieve its goals. Major government mission areas such as electronic benefits, electronic commerce, law enforcement, environmental protection, national defense, and health care may be represented on the Services Board to provide a program operations perspective. Initial selection of members will be made by OMB in consultation with other agencies as

appropriate. The CIO Council may nominate two members. The Services Board shall recommend new members to OMB for consideration. The Chair will be elected by the Services Board.

Sec. 5. Information Technology Resources Board.

(a) **Purpose and Functions.** An Information Technology Resources Board ("Resource Board") is established to provide independent assessments to assist in the development, acquisition, and management of selected major information systems and to provide recommendations to agency heads and OMB as appropriated. The Resources Board shall:

(1) review, at the request of an agency and OMB, specific information systems proposed or under development and make recommendations to the agency and OMB regarding the status of systems or next steps;

(2) publicize lessons learned and promising practices based on information systems reviewed by the Board; and

(3) seek the views of experts from industry, academia, and State and local governments on matters of concern to the Resources Board, as appropriate.

(b) **Membership.** The Resources Board shall be composed of individuals from executive branch agencies based on their knowledge of information technology, program, or acquisition management within Federal agencies. Selection of members shall be made by OMB in consultation with other agencies as appropriate. The Chair will be elected by the Resources Board. The Resources Board may call upon the department or agency whose project is being reviewed, or any other department or agency to provide knowledgeable representative(s) to the Board whose guidance and expertise will assist in focusing on the primary issue(s) presented by a specific system.

Sec. 6. Office of Management and Budget. The Director of OMB shall:

(1) evaluate agency information resources management practice and, as part of the budget process, analyze, track and evaluate the risks and results of all major capital investments for information systems;

(2) notify an agency if it believes that a major information system requires outside assistance;

(3) provide guidance on the implementation of this order and on the management of information resources to the executive agencies and to the Boards established by this order; and

(4) evaluate the effectiveness of the management structure set out in this order after 3 years and make recommendations for any appropriate changes.

Sec. 7. General Services Administration. Under the direction of OMB, the Administrator of General Services shall:

(1) continue to manage the FTS2000 program and coordinate the follow-on to that program, on behalf of and with the advice of customer agencies;

(2) develop, maintain, and disseminate for the use of the Federal community, as requested by OMB or the agencies, recommended methods and strategies for the development and acquisition of information technology;

(3) conduct and manage outreach programs in cooperation with agency managers;

(4) be a focal point for liaison on information resources management, including Federal information technology, with State and local governments, and with nongovernmental international organizations subject to prior consultation with the Secretary of State to ensure such liaison would be consistent with and support overall United States foreign policy objectives;

(5) support the activities of the Secretary of State for liaison, consultation, and negotiation with intergovernmental organizations in information resources management matters;

(6) assist OMB, as requested, in evaluating agencies' performance-based management tracking systems and agencies' achievement of cost, schedule, and performance goals; and

(7) provide support and assistance to the interagency groups established in this order.

Sec. 8. Department of Commerce. The Secretary of Commerce shall carry out the standards responsibilities under the Computer Security Act of 1987, as amended by the Information Technology Act, taking into consideration the recommendations of the agencies, the CIO Council, and the Services Board.

Sec. 9. Department of State. (a) The Secretary of State shall be responsible for liaison, consultation, and negotiation with foreign governments and intergovernmental organizations on all matters related to information resources management, including Federal information technology. The Secretary shall further ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international standards and recommendations affecting information technology. In the exercise of these responsibilities, the Secretary shall consult, as appropriate, with affected domestic agencies, organizations, and other members of the public.

(b) The Secretary of State shall advise the Director on the development of United States positions and policies on international information policy and technology issues affecting

Federal Government activities and the development of international information technology standards.

Sec. 10. Definitions (a) "Executive agency" has the meaning given to that term in section

4 (1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403 (1)).

(b) "Information Technology" has the meaning given that term in section 5002 of the Information Technology Act.

(c) "Information resources" has the meaning given that term in section 3502(6) of title 44, United States Code.

(d) "Information resources management" has the meaning given that term in section 3502(7) of title 44, Untied States Code.

(e) "Information system" has the meaning given that term in section 3502(8) of title 44, United States Code.

(f) "Affinity group" means any interagency group focused on a business or technology area with common information technology or customer requirements. The functions of an affinity group can include identifying common program goals and requirements; identifying opportunities for sharing information to improve quality and effectiveness; reducing costs and burden on the public; and recommending protocols and other standards, including security standards, to the National Institute of Standards and Technology for Government-wide applicability, for action in accordance with the Computer Security Act of 1987, as amended by the Information Technology Act.

(g) "National security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves crypto logic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Sec. 11. Applicability to National Security Systems.

The heads of executive agencies shall apply the policies and procedures established in this order to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in the Information Technology Act.

Sec. 12. Judicial Review. Nothing in this Executive order shall affect any otherwise available judicial review of agency action. This Executive order is intended only to improve the internal management of the executive branch and does not create any right or

benefit, substantive or procedural, enforceable at law or equity by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

William J. Clinton
THE WHITE HOUSE
July 16, 1996

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. PRESIDENTIAL DECISION DIRECTIVE 63

WHITE PAPER
The Clinton Administration's Policy on
Critical Infrastructure Protection:
Presidential Decision Directive 63
May 22, 1998

This White Paper explains key elements of the Clinton Administration's policy on critical infrastructure protection. It is intended for dissemination to all interested parties in both the private and public sectors. It will also be used in U.S. Government professional education institutions, such as the National Defense University and the National Foreign Affairs Training Center, for coursework and exercises on interagency practices and procedures. Wide dissemination of this unclassified White Paper is encouraged by all agencies of the U.S. Government.

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

II. President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

III. A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services;
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

IV. A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector. Together these two individuals and the departments and

corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;
- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies.

V. Guidelines

In addressing this potential vulnerability and the means of eliminating it, President Clinton wants those involved to be mindful of the following general principles and concerns.

- We shall consult with, and seek input from, the Congress on approaches and programs to meet the objectives set forth in this directive.
- The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.
- Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.
- The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, or providing information upon which choices can be made by the private sector. These incentives, along with other actions, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security.

- The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available, as appropriate, to ensure that critical infrastructure protection is achieved and maintained.

- Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably.

- The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.

- The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.

- We must focus on preventative measures as well as threat and crisis management. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.

- Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and actions shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

VI. Structure and Organization

The Federal Government will be organized for the purposes of this endeavor around four components (elaborated in Annex A).

1. Lead Agencies for Sector Liaison: For each infrastructure sector that could be a target for significant cyber or physical attacks, there will be a single U.S. Government department which will serve as the lead agency for liaison. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection and, in particular, in recommending components of the National Infrastructure Assurance Plan. Together, the Lead Agency and the private sector

counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.

2. Lead Agencies for Special Functions: There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, law enforcement). For each of those special functions, there shall be a Lead Agency which will be responsible for coordinating all of the activities of the United States Government in that area. Each lead agency will appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.

3. Interagency Coordination: The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will be appointed by and report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). Where appropriate, the CICG will be assisted by extant policy structures, such as the Security Policy Board, Security Policy Forum and the National Security and Telecommunications and Information System Security Committee.

4. National Infrastructure Assurance Council: On the recommendation of the Lead Agencies, the National Economic Council and the National Coordinator, the President will appoint a panel of major infrastructure providers and state and local government officials to serve as the National Infrastructure Assurance Council. The President will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to the President as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate.

VII. Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorizations.

No later than 180 days from issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical Infrastructure Coordination Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect critical infrastructure.

VIII. Tasks

Within 180 days, the Principals Committee should submit to the President a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

1. Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.

2. Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.

3. Warning: A national center to warn of significant infrastructure attacks will be established immediately (see Annex A). As soon thereafter as possible, we will put in place an enhanced system for detecting and

analyzing such attacks, with maximum possible participation of the private sector.

4. Response: A system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.
5. Reconstitution: For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly.

6. Education and Awareness: There shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.

7. Research and Development: Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.

8. Intelligence: The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat.

9. International Cooperation: There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.

10. Legislative and Budgetary Requirements: There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to the President as necessary. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB.

The CICG shall also review and schedule the taskings listed in Annex B.

IX. Implementation

In addition to the 180-day report, the National Coordinator, working with the National Economic Council, shall provide an annual report on the implementation of this directive to the President and the heads of departments and agencies, through the Assistant to the President for National Security Affairs. The report should include an updated threat

assessment, a status report on achieving the milestones identified for the National Plan and additional policy, legislative and budgetary recommendations. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. In addition, following the establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review.

Annex A: Structure and Organization

Lead Agencies: Clear accountability within the U.S. Government must be designated for specific sectors and functions. The following assignments of responsibility will apply.

Lead Agencies for Sector Liaison:

Commerce	Information and communications
Treasury	Banking and finance
EPA	Water supply
Transportation	Aviation Highways (including trucking and intelligent transportation systems) Mass transit Pipelines Rail Waterborne commerce
Justice/FBI	Emergency law enforcement services
FEMA	Emergency fire service Continuity of government services
HHS	Public health services, including prevention, surveillance, laboratory services and personal health services
Energy	Electric power Oil and gas production and storage

Lead Agencies for Special Functions:

Justice/FBI	Law enforcement and internal security
CIA	Foreign intelligence
State Foreign Affairs	
Defense	National defense

In addition, OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council. Furthermore, while Commerce is the lead agency for information and

communication, the Department of Defense will retain its Executive Agent responsibilities for the National Communications System and support of the President's National Security Telecommunications Advisory Committee.

National Coordinator: The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism shall be responsible for coordinating the implementation of this directive. The National Coordinator will report to the President through the Assistant to the President for National Security Affairs. The National Coordinator will also participate as a full member of Deputies or Principals Committee meetings when they meet to consider infrastructure issues. Although the National Coordinator will not direct Departments and Agencies, he or she will ensure interagency coordination for policy development and implementation, and will review crisis activities concerning infrastructure events with significant foreign involvement. The National Coordinator will provide advice, in the context of the established annual budget process, regarding agency budgets for critical infrastructure protection. The National Coordinator will chair the Critical Infrastructure Coordination Group (CICG), reporting to the Deputies Committee (or, at the call of its chair, the Principals Committee). The Sector Liaison Officials and Special Function Coordinators shall attend the CICG's meetings. Departments and agencies shall each appoint to the CICG a senior official (Assistant Secretary level or higher) who will regularly attend its meetings. The National Security Advisor shall appoint a Senior Director for Infrastructure Protection on the NSC staff.

A National Plan Coordination (NPC) staff will be contributed on a non-reimbursable basis by the departments and agencies, consistent with law. The NPC staff will integrate the various sector plans into a National Infrastructure Assurance Plan and coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. The NPC staff will also help coordinate a national education and awareness program, and legislative and public affairs.

The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the NPC, during the remainder of FY98. Beginning in FY99, the NPC shall be an office of the Commerce Department. The Office of Personnel Management shall provide the necessary assistance in facilitating the NPC's operations. The NPC will terminate at the end of FY01, unless extended by Presidential directive.

Warning and Information Centers

As part of a national warning and information sharing system, the President immediately authorizes the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, the

President also directs the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

National Infrastructure Protection Center (NIPC): The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.

All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law. The NIPC will include elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach and development and application of technical tools. In addition, it will establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create, such as the Information Sharing and Analysis Center described below.

The NIPC, in conjunction with the information originating agency, will sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity. Before disseminating national security or other information that originated from the intelligence community, the NIPC will coordinate fully with the intelligence community through existing procedures. Whether as sanitized or unsanitized reports, the NIPC will issue attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators. These warnings may also include guidance regarding additional protection measures to be taken by owners and operators. Except in extreme emergencies, the NIPC shall coordinate with the National Coordinator before issuing public warnings of imminent attacks by international terrorists, foreign states or other malevolent foreign powers.

The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. Depending on the nature and

level of a foreign threat/attack, protocols established between special function agencies (DOJ/DOD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DOD or the Intelligence Community.

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the National Coordinator, with the assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government. As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors.

Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.

Annex B: Additional Taskings

Studies

The National Coordinator shall commission studies on the following subjects:

- Liability issues arising from participation by private sector companies in the information sharing process.

- Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.

- The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who will misuse it.

- The improved protection, including secure dissemination and information handling systems, of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, it is unwise to disclose.

- The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of United States infrastructures.

- The potential benefit to security standards of mandating, subsidizing, or otherwise assisting in the provision of insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States.

Public Outreach

In order to foster a climate of enhanced public sensitivity to the problem of infrastructure protection, the following actions shall be taken:

- The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations.

- The National Academy of Sciences and the National Academy of Engineering shall consider a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.

- The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials.

- The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign; and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security.

Internal Federal Government Actions

In order for the Federal Government to improve its infrastructure security, these immediate steps shall be taken:

- The Department of Commerce, the General Services Administration, and the Department of Defense shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies.

- The National Coordinator shall coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and provide recommendations on how these institutions can cooperate most effectively.

- All federal agencies shall make clear designations regarding who may authorize access to their computer systems.

- The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure.

- The Federal Bureau of Investigation, the Secret Service and other appropriate agencies shall: (1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills for full-time employment as well as for part-time work with regional computer crime squads; and (2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks.

- The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.

- The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks.

- GSA shall identify large procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and propose, if necessary, revisions to the overall procurement process to do so.

- OMB shall direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Results Act strategic planning and performance measurement framework.

- The NSA, in accordance with its National Manager responsibilities in NSD-42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations. Assisting the Private Sector In order to assist the private sector in achieving and maintaining infrastructure security:

- The National Coordinator and the National Infrastructure Assurance Council shall propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems.

- The Department of Commerce and the Department of Defense shall work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.

- The Department of Justice and Department of the Treasury shall sponsor a comprehensive study compiling demographics of computer crime, comparing state approaches to computer crime and developing ways of deterring and responding to computer crime by juveniles.

LIST OF REFERENCES

Amburgey, Terry L., and Tina Dacin. 1994. "As the Left Foot Follows the Right? The Dynamics of Strategic and Structural Change." *Academy of Management Journal,* 37(6), 1427-1452.

Appleby, Joyce, Margaret Jacob, and Lynn Hunt. Telling the Truth about History. Norton, W. W. & Company, Inc., 1995.

Arquilla, John, and David Ronsfeldt, In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica, CA.: Rand, 1997.

Berger, Alexander *Organizational Innovation and Redesign in the Information Age: The Drug War, Net War and Other Lower-End Conflict,* Master's Thesis, Naval Postgraduate School, Monterey, CA, 1998.

Bolman, Lee, and Deal, Terrence. Reframing Organizations. San Francisco, CA: Jossey-Bass Publishers, 1991.

Brown, A. Bodyguard of Lies. New York, New York: Bantam Books, 1975.

Breuer, William B. Hoodwinking Hitler: The Normandy Deception. Westport, CT: Praeger Publishers, 1993.

Burton, R.M., and B. Obel, Strategic Organizational Diagnosis and Design: Developing a Theory for Application. Norwell, Mass: Kluwer Academic Publisher, 1998.

Choo, Chun Wei, Information Management for the Intelligent Organization. Medford NJ: Learned Information Inc. For the American Society For Information Science, 1998.

Central Intelligence Agency, http://www.cia.gov/

Czerwinski, Thomas J. "The Third Wave: What the Toffler's Never Told You." *NDU Strategic Forum,* Report Number 72, April 1996.

Director of Central Intelligence, http://www.odci.gov/

Environmental Protection Agency, http://www.epa.gov/

Erickson, Bo, "Organizational Design", Department of Organization, University of Southern Denmark, http://www.sam.sdu.dk/undervis/org-des, 2000.

Executive Office of the President. A National Security for a New Century. Washington, D.C., October 1998.

Executive Office of the President. A National Security for a New Century. Washington, D.C., October 1999.

Federal Emergency Management Agency, http://www.fema.gov/

Friedman, Thomas L., The Lexus and the Olive Tree. New York: Farrar, Straus and Giroux, 1999.

Galbraith, Jay R., "Organization Design." In J. Lorsch (ed.), *Handbook of Organization Behavior,* Englewood Cliffs, NJ: Prentice-Hall, 1987.

Galbraith, Jay R., "Organization Design: An Information Processing View", *Interfaces*, 4(3), pp. 28-36.

Galbraith, Jay R., Organization Design. Menlo Park, CA: Addison Wesley Publishing., 1977.

Garigue, R., *Information Warfare: Developing a Conceptual Framework,* Office of the Assistant Deputy Minister (Defense Information Services), http://www.cse.dnd.ca/~formis/overview/iw, 1995.

Gerblick, Thomas H. "IO for CINCs: Theory and Practice" USAWC Strategy Research Project, May 2000.

Hatcher, Robert V., advertisement in *Wall Street Journal,* June 6, 1989, p. A3.

Headquarters, Department of the Army, *Information Operations* (Field Manual 100-6), Washington DC: U.S. Government Printing Office, August 1996.

Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998.

Miller, Danny. 1987b. "Strategy Making and Structure: Analysis and Implications for Performance." *Academy of Management Journal,* 30(1), 7-32.

Morgan, Gareth, Images of Organization. Newbury, CA: Sage Publications, 1986.

Morgan, Gareth, Riding the Waves of Change. San Francisco, CA: Jossey-Bass Publishers, 1988.

National Defense Panel, Transforming Defense: National Security in the 21st Century. Arlington, Virginia. December 1997.

National Defense University, Information Age Anthology. Washington D.C.: 1997.

Nixon, Robert, "Information Technology and Knowledge Management," Department of Management, University of Southern Florida, http://www.coba.usf.edu/nixon, 2000.

Nonaka, Ikujiro, and Hirotaka Takeuchi, The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. New York: Oxford University Press, 1995.

Nuechterlein, Donald E., United States National Interests in a Changing World. Lexington, KY: University Press of Kentucky, 1973.

ORGCON v7.0, computer program in: Burton, R.M., and B. Obel, Strategic Organizational Diagnosis and Design: Developing a Theory for Application, Kluwer Academic Publisher, 1998.

Perrow, Charles, Complex Organizations: A Critical Essay. Glenview, Ill.: Scott, Foresman, and Co., 1972.

Posen, Barry R., The Sources of Military Doctrine. Ithaca, NY: Cornell University Press, 1984.

Robbins, Stephen P. 1990. Organization Theory: Structure, Design, and Applications. Englwood Cliffs, NJ: Prentice-Hall. (1st ed., 2nd ed., 1987).

Simon, Herbert A., The Science of the Artificial. Cambridge, MA: MIT Press, 1981.

Strange, Susan, States and Markets. London: Printer Publishers Limited, 1988.

Sun Tzu, The Art of War. Translated by Griffith, Samuel B. New York: Oxford University Press, 1963.

Taigiuri and George H. Litwin. 1968. "Organizational Climate." Harvard University.

Toffler, Alvin and Heidi. War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little, Brown, 1993.

U.S. Department of Agriculture, http://www.usda.gov/

U.S. Department of Commerce, http://www.doc.gov/

U.S. Department of Defense, http://www.defenselink.gov/

U.S. Department of Education, http://www.ed.gov/

U.S. Department of Energy, http://www.energy.gov/

U.S. Department of Health and Human Services, http://www.hhs.gov/

U.S. Department of Housing and Urban Development, http://www.hud.gov/

U.S. Department of the Interior, http://www.doi.gov/

U.S. Department of Justice, http://www.usdoj.gov/

U.S. Department of Labor, http://www.dol.gov/

U.S. Department of State, http://www.state.gov/

U.S. Department of the Treasury, http://www.treasury.gov/

U.S. Department of Transportation, http://www.dot.gov/

Van Der Spek, R. and R. De Hoog, Knowledge Management Methods: Practical Approaches to Managing Knowledge. Vol. 3 of 3. Arlington, Texas: Schema Press, 1995.

Zack, Michael H, "Developing a Knowledge Strategy", *California Management Review,* Vol. 41, No. 3, Spring 1999, pp. 125-145.

Zuboff, Shoshana, In the Age of the Smart Machine. New York, NY: Basic Books Inc, 1988.

BIBLIOGRAPHY

Amburgey, Terry L., and Tina Dacin. 1994. "As the Left Foot Follows the Right? The Dynamics of Strategic and Structural Change." *Academy of Management Journal,* 37(6), 1427-1452.

Appleby, Joyce, Margaret Jacob, and Lynn Hunt. Telling the Truth about History. Norton, W. W. & Company, Inc., 1995.

Arquilla, John "The Strategic Implications of Information Dominance," *Strategic Review*, Summer 1994, p. 28.

Arquilla, John, and David Ronsfeldt, In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica, CA.: Rand, 1997.

Berger, Alexander *Organizational Innovation and Redesign in the Information Age: The Drug War, Net War and Other Lower-End Conflict*, Master's Thesis, Naval Postgraduate School, Monterey, CA, 1998.

Bolman, Lee, and Terrance Deal, Reframing Organizations. San Franciso, CA: Jossey-Bass Publishers, 1991.

Brown, A., Bodyguard of Lies. New York, New York: Bantam Books, 1975.

Breuer, William B., Hoodwinking Hitler: The Normandy Deception. Westport, CT: Praeger Publishers, 1993.

Burton, R.M., and B. Obel, Strategic Organizational Diagnosis and Design: Developing a Theory for Application. Norwell, Mass: Kluwer Academic Publisher, 1998.

Choo, Chun Wei, Information Management for the Intelligent Organization. Medford NJ: Learned Information Inc. For the American Society For Information Science, 1998.

Central Intelligence Agency, http://www.cia.gov/

Czerwinski, Thomas J., "Command and Control at the Crossroads." Marine Corps Gazette, October 1995, 13-15.

Czerwinski, Thomas J., "The Third Wave: What the Toeffler's Never Told You." *NDU Strategic Forum,* Report Number 72, April 1996.

Director of Central Intelligence, http://www.odci.gov/

Drake, William J., The New Information Infrastructure: Strategies for US Policy. New York: The Twentieth Century Fund Press, 1995.

Environmental Protection Agency, http://www.epa.gov/

Erickson, Bo, "Organizational Design", Department of Organization, University of Southern Denmark, http://www.sam.sdu.dk/undervis/org-des, 2000.

Executive Office of the President, A National Security for a New Century. Washington, D.C., October 1998.

Executive Office of the President, A National Security for a New Century. Washington, D.C., October 1999.

Federal Emergency Management Agency, http://www.fema.gov/

Friedman, Thomas L., The Lexus and the Olive Tree. New York: Farrar, Straus and Giroux, 1999.

Galbraith, Jay R., "Organization Design." In J. Lorsch (ed.), Handbook of Organization Behavior. Englewood Cliffs, NJ: Prentice-Hall, 1987.

Galbraith, Jay R., "Organization Design: An Information Processing View", *Interfaces*, 4(3), pp. 28-36.

Galbraith, Jay R., Organization Design. Menlo Park, CA: Addison Wesley Publishing., 1977.

Garigue, R., *Information Warfare: Developing a Conceptual Framework,* Office of the Assistant Deputy Minister (Defense Information Services), http://www.cse.dnd.ca/~formis/overview/iw, 1995.

Gerblick, Thomas H. "IO for CINCs: Theory and Practice." USAWC Strategy Research Project, May 2000.

Guibault, R.G. "Information Empowerment: The Key Force Multiplier." Defense & Security Electronics, January 1996, 10, 14.

Hatcher, Robert V., advertisement in *Wall Street Journal,* June 6, 1989, p. A3.

Headquarters, Department of the Army, *Information Operations* (Field Manual 100-6), Washington DC: U.S. Government Printing Office, August 1996.

Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998.

Krepinevich, Andrew F., "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest*, Fall 1994, p. 30.

Metzgar, Terry. "Hostile Intercepts Aimed At Information Systems." National Defense, May-June 1993, 24-26.

Miller, Danny, 1987b. "Strategy Making and Structure: Analysis and Implications for Performance." *Academy of Management Journal,* 30(1), 7-32.

Morgan, Gareth, Images of Organization. Newbury, CA: Sage Publications, 1986.

Morgan, Gareth, Riding the Waves of Change. San Francisco, CA: Jossey-Bass Publishers, 1988.

Murphy, Dennis M. "Information Operations on the Nontraditional Battlefield." Military Review, November-December 1996, 16-18.

National Defense Panel, Transforming Defense: National Security in the 21st Century. Arlington, Virginia. December 1997.

National Defense University, Information Age Anthology. Washington D.C.: 1997.

Nifong, Michael R. "The Key to Information Dominance." Military Review, May-June 1996, 62-67.

Nixon, Robert, "Information Technology and Knowledge Management," Department of Management, University of Southern Florida, http://www.coba.usf.edu/Nixon, 2000.

Nonaka, Ikujiro, and Hirotaka Takeuchi, The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. New York: Oxford University Press, 1995.

Nuechterlein, Donald E., United States National Interests in a Changing World. Lexington, KY: University Press of Kentucky, 1973.

Office of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, D.C.: 1984), p. 188.

Office of the Joint Chiefs of Staff, *Doctrine for Joint Operations*, Joint Publication 3-0 (Washington, D.C.: 1995), p. III-20.

ORGCON v7.0, computer program in: Burton, R.M., and B. Obel, Strategic Organizational Diagnosis and Design: Developing a Theory for Application, Kluwer Academic Publisher, 1998.

Orr, Joseph E. Information Dominance: A Policy of Selective Engagement. Carlisle Barracks, PA: AWC, 1997.

Owens, Admiral William A. "Emerging System of Systems." US Naval Institute Proceedings, May 1995, 3539.

Perrow, Charles, Complex Organizations: A Critical Essay. Glenview, Ill.: Scott, Foresman, and Co., 1972.

Posen, Barry R., The Sources of Military Doctrine. Ithaca, NY: Cornell University Press, 1984.

Robbins, Stephen P. 1990. Organization Theory: Structure, Design, and Applications. Englwood Cliffs, NJ: Prentice-Hall, 1987.

Ronfeldt, David F. Cyberocracy, Cyberspace, And Cyberology: Political Effects of the Information Revolution. Santa Monica, CA: RAND Corporation, 1991.

Ryan, Donald E. Jr., "Implications of Information-Based Warfare," *Joint Force Quarterly*, Autumn/Winter 1994-95; p. 114.

Simon, Herbert A., The Science of the Artificial. Cambridge, MA: MIT Press, 1981.

Strange, Susan, States and Markets. London: Printer Publishers Limited, 1988.

Sun Tzu, The Art of War. Translated by Samuel B Griffith. New York: Oxford University Press, 1963.

Taigiuri and George H. Litwin, "Organizational Climate." Harvard University, 1968.

Tempestilli, Mark. "Network Force." *US Naval Institute Proceedings*, June 1996, 42-46.

Toeffler, Alvin and Heidi. War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little, Brown, 1993.

Thompson, Michael J. Information Warfare—Who is Responsible?: Coordinating the Protection of Our National Information Infrastructure. Carlisle Barracks, PA: AWC, 1997.

U.S. Department of Agriculture, http://www.usda.gov/

U.S. Department of Commerce, http://www.doc.gov/

U.S. Department of Defense, http://www.defenselink.gov/

U.S. Department of Education, http://www.ed.gov/

U.S. Department of Energy, http://www.energy.gov/

U.S. Department of Health and Human Services, http://www.hhs.gov/

U.S. Department of Housing and Urban Development, http://www.hud.gov/

U.S. Department of the Interior, http://www.doi.gov/

U.S. Department of Justice, http://www.usdoj.gov/

U.S. Department of Labor, http://www.dol.gov/

U.S. Department of State, http://www.state.gov/

U.S. Department of the Treasury, http://www.treasury.gov/

U.S. Department of Transportation, http://www.dot.gov/

Van Der Spek, R. and De Hoog, R., Knowledge Management Methods: Practical Approaches to Managing Knowledge. Vol. 3 of 3. Arlington, Texas: Schema Press, 1995.

Zack, Michael H, "Developing a Knowledge Strategy", *California Management Review,* Vol. 41, No. 3, Spring 1999, pp. 125-145.

Zuboff, Shoshana, In the Age of the Smart Machine. New York, NY: Basic Books Inc, 1988.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, Virginia 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, California 93943-5101

3. Professor Carl R. Jones 1
   Code IS/JS
   Naval Postgraduate School
   Monterey, CA 93940

4. COL Thomas H. Gerblick 1
   Department of State
   SA 44 / IIP / T / PS
   Washington, DC 20520

5. LT Ray Buettner 2
   Code IW
   Naval Postgraduate School
   Monterey, CA 93940

6. LT Richard Dougherty 3
   10 Bay Path Ct
   Huntington, NY 11743

7. LT Pablo Mir 3
   PO Box 872
   McLean, VA 22101

8. MAJ Mark W. Garrett 1
   1107 East 13th Street
   Big Spring, TX 79720